S. Hrg. 99-1006

ELECTRONIC COMMUNICATION PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON
PATENTS, COPYRIGHTS AND TRADEMARKS

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

NINETY-NINTH CONGRESS

FIRST SESSION

ON

S. 1667

A BILL TO AMEND TITLE 18, UNITED STATES CODE, WITH RESPECT TO THE INTERCEPTION OF CERTAIN COMMUNICATIONS, OTHER FORMS OF SURVEILLANCE, AND FOR OTHER PURPOSES

WEDNESDAY, NOVEMBER 13, 1985

Serial No. J-99-72

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
57-910 O WASHINGTON : 1987

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

5521-27

COMMITTEE ON THE JUDICIARY

STROM THURMOND, South Carolina, *Chairman*

CHARLES McC. MATHIAS, Jr., Maryland
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ALAN K. SIMPSON, Wyoming
JOHN P. EAST, North Carolina
CHARLES E. GRASSLEY, Iowa
JEREMIAH DENTON, Alabama
ARLEN SPECTER, Pennsylvania
MITCH McCONNELL, Kentucky

JOSEPH R. BIDEN, Jr., Delaware
EDWARD M. KENNEDY, Massachusetts
ROBERT C. BYRD, West Virginia
HOWARD M. METZENBAUM, Ohio
DENNIS DeCONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois

Dennis W. Shedd, *Chief Counsel and Staff Director*
Diana L. Waterman, *General Counsel*
Deborah G. Bernstein, *Chief Clerk*
Mark H. Gitenstein, *Minority Chief Counsel*

Subcommittee on Patents, Copyrights and Trademarks

CHARLES McC. MATHIAS, Jr., Maryland, *Chairman*

PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ALAN K. SIMPSON, Wyoming

PATRICK J. LEAHY, Vermont
HOWARD M. METZENBAUM, Ohio
DENNIS DeCONCINI, Arizona

Steven J. Metalitz, *Chief Counsel and Staff Director*
Pamela S. Batstone, *Chief Clerk*
John D. Podesta, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

Page
Mathias, Hon. Charles McC., Jr., a U.S. Senator from the State of Maryland, chairman, Subcommittee on Patents, Copyrights and Trademarks 1, 2
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 40, 42

PROPOSED LEGISLATION

S. 1667, a bill to amend title 28, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes 4

CHRONOLOGICAL LIST OF WITNESSES

Kastenmeier, Hon. Robert W., a U.S. Representative in Congress from the State of Wisconsin; and Hon. Carlos J. Moorhead, a U.S. Representative in Congress from the State of California 32
Knapp, James, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, accompanied by Harry Myers, associate chief counsel, Drug Enforcement Administration; and Frederick Hess, Director, Office of Enforcement Operations, Criminal Division, U.S. Department of Justice 44
Walker, Philip M., vice chairman, Electronic Mail Association, Washington, DC; P. Michael Nugent, chairman, Committee on Computer Systems and Communications Privacy, Association of Data Processing Service Organizations, Arlington, VA; and John Stanton, chairman, Telocator Network of America, Washington, DC 93
Berman, Jerry J., chief legislative counsel, American Civil Liberties Union, Washington, DC, and Lynn W. Ellis, chairman, Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers, Washington, DC, accompanied by P. Howard Patrick 124

ALPHABETICAL LIST AND MATERIAL SUBMITTED

Berman, Jerry J.:
    Testimony 124
    Prepared statement 129
Ellis, Lynn W.:
    Testimony 135
    Prepared statement 138
    Proposed changes in wording of S. 1667 and reasons for changing 141
Hess, Frederick:
    Testimony 71
    "Prosecutive Results Obtained in Investigations Utilizing Electronic Surveillance (Wiretaps)," survey prepared by: Office of Enforcement Operations, Criminal Division, Department of Justice, April 25, 1986 83
Kastenmeier, Hon. Robert W.:
    Testimony 32
    Prepared statement 34
Knapp, James:
    Testimony 44
    Prepared statement 49
Mathias, Hon. Charles McC., Jr.: "Electronic Surveillance and Civil Liberties," excerpt from OTA report 65
Moorhead, Hon. Carlos J.: Testimony 36

Page

Nugent, P. Michael:
  Testimony ... 100
  Prepared statement ... 103
  Letter to Senator Mathias, October 8, 1986 ... 109
Stanton, John:
  Testimony ... 113
  Prepared statement ... 115
Walker, Philip M.:
  Testimony ... 93
  Prepared statement ... 96

APPENDIX

DOCUMENTS REFLECTING DEVELOPMENTS ON THE ELECTRONIC COMMUNICATIONS PRIVACY ACT SUBSEQUENT TO THE HEARING ON S. 1667

Statement of Senator Charles McC. Mathias, Jr., markup session on S. 2575, August 12, 1986 ... 149
A summary of the Electronic Communications Privacy Act ... 152
Supporters of H.R. 4952, the Electronic Communications Privacy Act ... 155
Summary of changes between H.R. 3378 and H.R. 4952, June 10, 1986 ... 156
"Telecommunications Privacy and Our Freedom," a lecture by Mortin S. Bromfield, May 14, 1986, cosponsored by the American Privacy Foundation and the Boston Public Library ... 158
Statement of Tandy Corp. on S. 1667, the Electronic Communications Privacy Act of 1985, December 13, 1985 ... 171
Preliminary statement of Perry F. Williams, secretary of the American Radio Relay League, Inc., on S. 1667, the Electronic Communications Privacy Act of 1985, December 1985 ... 179

CORRESPONDENCE

Letter to Senator Mathias, with statement on S. 1667 by the Personal Radio Steering Group, Inc., November 25, 1985 ... 184
Letters to Senator Strom Thurmond, chairman, Committee on the Judiciary, from:
  John R. Bolton, Assistant Attorney General, U.S. Department of Justice, June 25, 1986 ... 190
  William A. Russell, Jr., Director, Office of Congressional and Public Affairs, Federal Communications Commission, July 30, 1986 ... 191
    Attachments:
      Copy of H.R. 4983, a bill to amend chapter 65 of title 18, United States Code, to provide a criminal penalty for interference with satellite communications ... 198
      Version of the proposed amendment (with Congressional Record statement), introduced as H.R. 4983 by Representative Howard Coble, June 11, 1986 ... 193

ELECTRONIC COMMUNICATION PRIVACY

WEDNESDAY, NOVEMBER 13, 1985

U.S. Senate,
Subcommittee on Patents,
Copyrights and Trademarks,
Committee on the Judiciary,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:38 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Charles McC. Mathias, Jr. (chairman of the subcommittee) presiding.

Also present: Senator Leahy.

Staff present: Steven J. Metalitz, staff director and acting chief counsel; Kenneth E. Mannella, counsel; Pamela S. Batstone, chief clerk; and John D. Podesta, minority chief counsel.

OPENING STATEMENT OF HON. CHARLES McC. MATHIAS, JR., A U.S. SENATOR FROM THE STATE OF MARYLAND, CHAIRMAN, SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS

Senator **Mathias**. The subcommittee will come to order.

Today, for the first time in the 99th Congress, the Subcommittee on Patents, Copyrights and Trademarks will examine the question of privacy. It is the first exercise during this Congress of our jurisdiction over privacy matters.

The hearing arises as a result of Senate bill 1667, the Electronic Communications Privacy Act of 1985. This is a bill introduced by Senator Leahy and myself which seeks to bring our laws up to date to meet the challenges to privacy posed by modern communications technology.

Because I am aware that Mr. Kastenmeier is under pressure of time, I am going to put the rest of my statement in the record and ask him if he will give us the benefit of his views and opinions.

[The prepared statement of Senator Mathias and a copy of S. 1667 follow:]

PREPARED STATEMENT OF SENATOR CHARLES McC. MATHIAS, JR.

Today, for the first time in the 99th Congress, the Subcommittee on Patents, Copyrights and Trademarks holds a hearing in the exercise of its jurisdiction over privacy legislation. Our topic is S. 1667, the Electronic Communications Privacy Act of 1985. This bill, which Senator Leahy and I introduced on September 19, seeks to bring our laws up to date with the new challenges to privacy posed by modern communications technology.

Just a few years ago, our nation's communications networks, while extensive, were relatively simple in form. The mails, the telegraph system, the telephone, and radio communications each played a role; but those roles were distinct from one another, and not too hard to understand. Those simple days are gone forever. Today's systems of electronic communication envelop our society in an invisible web, complex in structure and pervasive in scope. We entrust, each day, to that network of electrons a wide spectrum of information, from the latest stock quotations to our most personal revelations. But the uneasy realization is growing that someone else may be listening. Modern technology, which has given us these dazzling new means of communications, has also opened up opportunities for new and more intrusive forms of snooping.

That is the problem that S. 1667 seeks to address. Just as our outdated models for understanding communications technology must be discarded, so we must move beyond the current statutory framework for safeguarding the right to privacy in these new communications media. That framework, last revised seventeen years ago with the passage of the federal wiretap statute, needs to be adapted to the new ways that Americans are using to communicate with each other and with the world.

Because the media that carry our messages have become so complex, it is not surprising that the legislation before us is complicated, too. Our hearings this morning mark our first opportunity to examine the provisions of S. 1667, and to hear the views of knowledgeable witnesses from both the government and the private sector. We look forward to learning more, both about the remarkable technology that has revolutionized the way we communicate, and about the legal pitfalls that we may encounter in the attempt to provide legal protection for the privacy of these new means of communication. But I hope that neither the technological buzzwords nor the legal flyspecking will obscure the need for legislative action in this field. The threat to privacy is as close to us as the telephones in our homes, our offices, and --- increasingly -- our cars. It is as inescapable as the computer terminals that are becoming a fixture of the way we work, learn and play. And it is as insistent as the paging devices that more and more of us are carrying. Our laws must respond to that threat, and S. 1667 represents a good start on that response.

We look forward with particular interest to hearing the views of the Justice Department. When Attorney General Meese appeared before the Judiciary Committee for confirmation, he singled out as one of his top priorities "the safeguarding of individual privacy from improper governmental intrusion." I believe S. 1667 is the most important legislative initiative in the field of privacy to come before the Senate since the Attorney General took office, so the Department's comments and suggestions are especially welcomed.

We will also hear testimony this morning from representatives of five organizations with lively interests in the subject matter of S. 1667: three associations of businesses that provide electronic communications services; the professional organization of electronic engineers; and the American Civil Liberties Union.

To open our hearing, we will welcome the chairman and the ranking minority member of our counterpart subcommittee in the House of Representatives, Robert Kastenmeier and Carlos Moorhead. They are also the principal sponsors of the companion legislation in the other body, H. R. 3378, on which hearings have already begun before the Subcommittee on Courts, Civil Liberties and the Administration of Justice.

Before we hear from Representatives Kastenmeier and Moorhead, I will yield to the ranking minority member of this subcommittee, who is also the principal sponsor of this legislation in the Senate. Senator Leahy's interest in this important problem of privacy in electronic communications has been an essential factor in bringing about this hearing.

II

99TH CONGRESS
1ST SESSION

S. 1667

To amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 19 (legislative day, SEPTEMBER 16), 1985

Mr. LEAHY (for himself and Mr. MATHIAS) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1985".

TITLE I—TITLE 18 AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510 of title 18, United States Code, is amended by striking out paragraph (1) and inserting in lieu thereof the following:

"(1) 'electronic communication' means any transmission of signs, signals, writing, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, or photoelectric system that affects interstate or foreign commerce;".

(2) Section 2510(4) of title 18, United States Code, is amended by striking out "aural acquisition" and inserting "interception" in lieu thereof.

(3) Section 2510(8) of title 18, United States Code, is amended by striking out "existence,".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter for any person—

"(i) to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public.

"(ii) to intercept any electronic communication which is transmitted—

"(I) by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress;

"(II) by a walkie talkie, or a police or fire communication system readily accessible to the public; or

"(III) by an amateur radio station operator or by a citizens band radio operator; or

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communication Act of 1934; or

"(II) is excepted from the application of section 705(a) of the Communication Act of 1934 by section 705(b) of that Act.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register (as that term is defined for the purposes of chapter 206 (relating to pen registers) of this title); or

"(ii) for a provider of electronic communication service to record the placement of a telephone call in order to protect such provider, or a user of that service, from abuse of service.".

(c) Technical and Conforming Amendments.—(1) Chapter 119 of title 18, United States Code, is amended by striking out "wire" each place it appears (including in any section heading) and inserting "electronic" in lieu thereof.

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "**AND OTHER ELECTRONIC COMMUNICATION**" after "**WIRE**".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "**and other electronic communication**" after "**Wire**".

(4) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "communication common carrier" and inserting "a provider of electronic communication service" in lieu thereof;

(B) by striking out "of the carrier" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": *Provided,* That said communication common carriers" and inserting ", except that a provider of electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "communication common carriers" and inserting "providers of electronic communication services" in lieu thereof; and

(B) by striking out "communication common carrier" each place it appears and inserting "provider of electronic communication services" in lieu thereof.

(6) Section 2512(2)(a) of title 18, United States Code, is amended—

(A) by striking out "communications common carrier" the first place it appears and inserting "a provider of an electronic communication service" in lieu thereof;

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that electronic communication service" in lieu thereof.

SEC. 102. ADDITIONAL PROHIBITIONS RELATING TO ELECTRONIC COMMUNICATIONS AND REQUIREMENTS FOR CERTAIN DISCLOSURES.

(a) Additional Prohibitions.—Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3) Unless authorized by the person or entity providing an electronic communication service or by a user of that service, and except as otherwise authorized in section 2516 of this title, whoever willfully accesses an electronic communication system through which such service is provided or willfully exceeds an authorization to access that electronic communication service and obtains or alters that electronic communication while it is stored in such system shall—

"(A) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(i) be fined not more than $250,000 or imprisoned not more than one year, or both, in the case of a first offense under this subparagraph;

"(ii) be fined not more than $250,000 or imprisoned not more than two years, or both, for any subsequent offense under this subparagraph; and

"(B) be fined not more than $5,000 or imprisoned not more than six months, or both, in any other case.

"(4) A person or entity providing an electronic communication service shall not knowingly divulge the contents of any communication (other than one to such person or entity) carried on that service to any person or entity other than the addressee of such communication or that addressee's agent, except—

"(A) as otherwise authorized in section 2516 of this title;

"(B) with the consent of the user originating such communication;

"(C) to a person employed to forward such communication to its destination; or

"(D) for a business activity related to a service provided by the provider of the electronic communication service to a user of the electronic communication service.".

(b) REQUIREMENTS FOR CERTAIN DISCLOSURES.—(1) Section 2516 of title 18, United States Code, is amended by adding at the end the following:

"(3) A person authorized to make application under this section for an interception may also make an application for a disclosure which would otherwise be in violation of section 2511 (3) or (4). Such application shall meet the requirements for an application for an interception under this section. The court shall not grant such disclosure unless the applicant demonstrates that the particular communications to be disclosed concern a particular offense enumerated in section 2516 of this title. If an order of disclosure is granted, disclosure of information under that order shall not be subject to the prohibitions contained in such section 2511 (3) or (4). Such disclosure shall be treated for the purposes of this chapter as interceptions under this chapter, and shall be subject to the same requirements and procedures as apply under this chapter to interceptions under this chapter.

"(4) A provider of electronic communication service may not, upon the request of a governmental authority, disclose to that authority a record kept by that provider in the course of providing that communication service and relating to a particular communication made through that service, unless the governmental authority obtains a court order for such disclosure based on a finding that—

"(A) the governmental entity reasonably suspects the person or entity by whom or to whom such communication was made to have engaged or to be about to engage in criminal conduct; and

"(B) the record may contain information relevant to that conduct.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) Any person whose electronic communication or oral communication is intercepted, accessed, disclosed, or used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) The court may assess as damages in an action under this section either—

"(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(2) statutory damages in an amount not less than $500 or more than $10,000.

"(d) A good faith reliance on a court warrant or order is a complete defense against a civil action under this section.

"(e) A civil action under this section may not be commenced later than two years after whichever is later of—

"(1) the date of the occurrence of the violation; or

"(2) the date upon which the claimant first has had a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY ACTING ASSISTANT ATTORNEY GENERAL.

Section 2516(1) of title 18 of the United States Code is amended by inserting "(or acting Assistant Attorney General)" after "Assistant Attorney General".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

Section 2516(1)(c) of title 18 of the United States Code is amended—

(1) by inserting "section 751 (relating to escape)," after "wagering information)";

(2) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(3) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),"; and

(4) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),".

SEC. 106. ADDITIONAL REQUIREMENTS FOR APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) INVESTIGATION OBJECTIVES.—Section 2518(1)(b) of title 18 of the United States Code is amended by inserting immediately before the semicolon at the end the following: ", and (v) the specific investigative objectives and the specific targets, if known, of the interception to which the application pertains".

(b) ALTERNATE INVESTIGATIVE TECHNIQUES.—Section 2518(1)(c) of title 18 of the United States Code is amended by inserting "(including the use of consensual monitoring, pen registers, tracking devices, contempt proceedings, perjury prosecutions, use of accomplice testimony, grand jury subpoena of documents, search warrants, interviewing witnesses, and obtaining documents through other legal means)" after "procedures".

(c) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device installed within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(d) REIMBURSEMENT FOR ASSISTANCE; PHYSICAL ENTRY.—Section 2518(4) of title 18 of the United States Code is amended—

(1) by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance"; and

(2) by adding at the end "An order authorizing the interception of an electronic communication under this chapter may, upon a showing by the applicant that there are no other less intrusive means reasonably available of effecting the interception, authorize physical entry by law enforcement officers to install an electronic, mechanical, or other device. No such order may require the participation of any individuals operating or employed by an electronic communications system in such physical entry.".

(e) PERIODIC REPORTS.—Subsection (6) of section 2518 of title 18 of the United States Code is amended to read as follows:

"(6) An order authorizing interception pursuant to this chapter shall require that reports be made not less often than every ten days to the judge who issued such order, showing what progress has been made toward achievement of the authorized objective, the need, if any for continued interception, and whether any evidence has been discovered through such interception of offenses other than those with respect to which such order was issued. The judge may suspend or terminate interception if any such report is deficient or evinces serious procedural irregularities. The judge shall terminate interception if the legal basis of continued interception no longer exists.".

(f) TIME LIMIT FOR THE MAKING AVAILABLE TO JUDGE OF RECORDINGS.—Section 2518(8)(a) of title 18 of the United States Code is amended by striking out "Immediately upon" and inserting "Not later than forty-eight hours after" in lieu thereof.

SEC. 107. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE II—PEN REGISTERS AND TRACKING DEVICES

SEC. 201. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS AND TRACKING DEVICES

"Sec.
"3121. General prohibition on pen register and tracking device use; exception.
"3122. Application for an order for a pen register or tracking device.
"3123. Issuance of an order for a pen register or tracking device.
"3124. Emergency use of pen register or tracking device without prior authorization.
"3125. Assistance in installation and use of a pen register or tracking device.

"3126. Notice to affected persons.
"3127. Reports concerning pen registers and tracking devices.
"3128. Recovery of civil damages authorized.
"3129. Definitions for chapter.

"§ 3121. General prohibition on pen register and tracking device use; exception

"(a) IN GENERAL.—Except as provided in this section or section 3124 of this title, no person may install or use a pen register or a tracking device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic communication services relating to the operation, maintenance, and testing of an electronic communication service.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined not more than $100,000 or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register or tracking device

"(a) LAW ENFORCEMENT OFFICERS MAY MAKE APPLICATION.—(1) A Federal law enforcement officer having responsibility for an ongoing criminal investigation may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a tracking device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) A State law enforcement officer having responsibility for an ongoing criminal investigation may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a tracking device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) CONTENT OF APPLICATION.—An application under subsection (a) of this section shall include—

"(1) the identity of the law enforcement officer making the application and of any other officer or employee authorizing or directing such application, and the identity of the agency in which each such law enforcement officer and other officer or employee is employed; and

"(2) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that an order should be issued.

"§ 3123. Issuance of an order for a pen register or tracking device

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court may enter an ex parte order, as requested or as found warranted by the court, authorizing or approving the installation and use of a pen register or a tracking device within the jurisdiction of the court (and outside that jurisdiction but within the United States in the case of a mobile tracking device installed within such jurisdiction) if the court finds on the basis of the information submitted by the applicant that—

"(1) in the case of a pen register, there is reasonable cause to believe; and

"(2) in the case of a tracking device, there is probable cause to believe;

that the information likely to be obtained by such installation and use is relevant to a legitimate criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased, in whose name is listed, or who commonly uses the telephone line to which the pen register is to be attached or of the person to be traced by means of the tracking device;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number of the telephone line to which the pen register is to be attached, or the identity of the object to which the tracking device is to be attached;

"(D) a statement of the nature of the criminal investigation to which the information likely to be obtained by the pen register or tracking device relates;

"(E) the identity of the law enforcement officer authorized to install and use the pen register or tracking device; and

"(F) the period of time during which the use of the pen register or tracking device is authorized; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register or tracking device under section 3125 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section may authorize or approve the installation and use of a pen register or tracking device for the period necessary to achieve the objective of the authorization, or for thirty days, whichever is less.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection

(a) of this section. The extension shall include a full and complete statement of any changes in the information required by subsection (b) of this section to be set forth in the original order. The period of extension may be for the period necessary to achieve the objective for which it was granted, or for thirty days, whichever is less.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER OR TRACKING DEVICE.—An order authorizing or approving the installation and use of a pen register or tracking device shall direct that the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, shall not disclose the existence of the pen register or tracking device until at least sixty days after its removal. Upon the request of the applicant, the court may order such person to postpone any disclosure of the existence of the pen register or tracking device for additional periods of not more than sixty days each, if the court finds, upon the showing of the applicant, that there is reason for the belief that disclosing the existence of the pen register or tracking device may—

"(1) endanger the life or physical safety of any person;

"(2) result in flight from prosecution;

"(3) result in destruction of, or tampering with, evidence;

"(4) result in intimidation of potential witnesses; or

"(5) otherwise seriously jeopardize an investigation or governmental proceeding.

"§ 3124. Emergency use of pen register or tracking device without prior authorization

"(a) In General.—A law enforcement officer specially designated by the Attorney General may install and use a pen register or a tracking device without a court order, if a judge of competent jurisdiction is notified at the time the decision to make such installation and use is made, and if—

"(1) such law enforcement officer reasonably determines that—

"(A) an emergency situation exists that involves—

"(i) immediate danger of death or serious bodily injury to any person;

"(ii) conspiratorial activities threatening the national security interest; or

"(iii) conspiratorial activities characteristic of organized crime;

that requires the installation and use of a pen register or a tracking device before an order authorizing the installation and use of the pen register or tracking device can, with due diligence, be obtained; and

"(B) there are grounds upon which an order could be entered under section 3123 of this title to authorize the installation and use of such pen register or tracking device; and

"(2) an application for an order approving the installation and use of the pen register or tracking device is made under section 3122 of this title as soon as practicable but not more than forty-eight hours after the pen register or tracking device is installed.

"(b) TERMINATION.—In the absence of an order approving the pen register or tracking device, the use of the pen register or tracking device shall terminate immediately when the information sought is obtained, or when the application for the order is denied, whichever is earlier.

"§ 3125. Assistance in installation and use of a pen register or tracking device

"(a) IN GENERAL.—Except as provided in subsection (b), upon the request of a law enforcement officer authorized by this chapter to install and use a pen register or tracking device, a communications common carrier, landlord, custodian, or other person shall furnish such law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register or tracking device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if—

"(1) such assistance is directed by a court order as provided in section 3123(b)(2) of this title; or

"(2) the emergency installation and use of the pen register or tracking device is authorized under section 3124 of this title.

"(b) EXCEPTION.—A law enforcement officer may not request the participation under this section of any individuals operating or employed by an electronic communications system in such physical entry.

"(c) COMPENSATION.—A communications common carrier, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be compensated for such assistance for reasonable expenses incurred in providing such facilities or assistance.

"§ 3126. Notice to affected persons

"(a) SERVICE OF INVENTORY.—Except as provided in subsection (b), within a reasonable time but not later than ninety days after the filing of an application for an order of approval required under section 3124 of this title, if such application is denied, or the termination of an order, as extended, under section 3123 of this title, the issuing or denying judge shall cause to be served on the persons named in the order or application, and such other parties to activity monitored by means of a pen register or tracking device as the judge may determine in the judge's discretion that it is in the interest of justice, an inventory which shall include notice of—

"(1) the fact of the entry of the order or the application;

"(2) the date of such entry and the period of authorized, approved, or disapproved activity under such order, or the denial of the application; and

"(3) the fact that during the period activity took place under such order.

"(b) EXCEPTION.—On an ex parte showing of good cause to a judge of competent jurisdiction—

"(1) the serving of the inventory required by this subsection may be postponed; and

"(2) the serving of such inventory may be dispensed with if notice under this section would compromise an ongoing criminal investigation or result in the disclosure of classified information harmful to the national security.

"(c) MOTION FOR INSPECTION.—The judge, upon the filing of a motion, may in the judge's discretion make available to such person or such person's counsel for inspection such portions of the results of activity under such order or referred to in such application, and such orders and applications as the judge determines to be in the interest of justice.

"§ 3127. Reports concerning pen registers and tracking devices

"(a) REPORT BY ISSUING OR DENYING JUDGE.—Within thirty days after the expiration of an order (or each extension thereof) entered under section 3123 of this title, or the denial of an order approving the use of a pen register or a tracking device, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

"(1) the fact that an order or extension was applied for;

"(2) the kind of order or extension applied for;

"(3) the fact that the order or extension was granted as applied for, was modified, or was denied;

"(4) the period of operation of the pen register or tracking device authorized by the order, and the number and duration of any extensions of the order;

"(5) the offense specified in the order or application, or extension of an order;

"(6) the identity of the applying law enforcement officer and agency making the application and the person authorizing the application; and

"(7) the nature of the facilities from which or the place where activity under the order was to be carried out.

"(b) REPORT BY ATTORNEY GENERAL.—In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

"(1) the information required by paragraphs (1) through (7) of subsection (a) of this section with respect to each application for an order or extension made during the preceding calendar year;

"(2) a general description of the pen registers and tracking devices conducted under such order or extension, including—

"(A) the approximate nature and frequency of incriminating evidence obtained;

"(B) the approximate number of persons whose activities were monitored; and

"(C) the approximate nature, amount, and cost of the manpower and other resources used in carrying out orders under this chapter;

"(3) the number of arrests resulting from activity conducted under such order or extension, and the offenses for which arrests were made;

"(4) the number of trials resulting from such activity;

"(5) the number of motions to suppress made with respect to such activity, and the number granted or denied;

"(6) the number of convictions resulting from such activity and the offenses for which the convictions were obtained and a general assessment of the importance of such activity; and

"(7) the information required by paragraphs (2) through (6) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

"(c) REPORT BY DIRECTOR OF ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders under this chapter and the number of orders and extensions granted or denied under this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (a) and (b) of this section.

The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (a) and (b) of this section.

"§ 3128. Recovery of civil damages authorized

"(a) Any person who is harmed by a violation of this chapter may in a civil action recover from the peson or entity which engaged in that violation such relief as may be appropriate.

"(b) In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) A good faith reliance on a court warrant or order is a complete defense against a civil action under this section.

"(d) A civil action under this section may not be commenced later than two years after whichever is later of—

"(1) the date of the occurrence of the violation; or

"(2) the date upon which the claimant first has had a reasonable opportuntiy to discover the violation.".

"§ 3129. Definitions for chapter

"As used in this chapter—

"(1) the term 'communications common carrier' has the meaning set forth for the term 'common carrier' in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

"(2) the term 'electronic communication' has the meaning set forth for such term in section 2510 of this title;

"(3) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by a statute of that State to enter orders authorizing the use of pen registers and tracking devices in accordance with this chapter;

"(4) the term 'legitimate criminal investigation' means a lawful investigation or official proceeding inquiring into a violation of any Federal criminal law;

"(5) the term 'pen register' means a device which records and or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider of electronic communication services for billing, or recording as an incident to billing, for communications services provided by such provider;

"(5) the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object in circumstances in which there exists a reasonable expectation of privacy with respect to such tracking; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers and Tracking Devices .... 3121".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect on the date of the enactment of this Act.

○

Senator **Mathias**. I believe Mr. Moorhead is going to appear with Mr. Kastenmeier. It is a great honor for us to have two Members of the House of Representatives, who are perhaps the most knowledgeable and who spend the most time and give the most thought to these subjects.

So we appreciate their being with us and we want to accommodate their schedules as much as it is possible.

STATEMENT OF A PANEL, CONSISTING OF HON. ROBERT W. KASTENMEIER, A U.S. REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN; AND HON. CARLOS J. MOORHEAD, A U.S. REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. **Kastenmeier**. Thank you, Mr. Chairman. We do appreciate that courtesy. It is a distinct honor and pleasure to appear before you this morning. Each of us here has spent a great amount of time over the past several Congresses attempting to reconcile the Federal law with the challenges of new and emerging technologies.

Indeed, your own subcommittee has made a magnificent contribution in that connection. The Semi-Conductor Chip Protection Act exemplifies our success in the intellectual property area.

The bill before you today, S. 1667, the Electronic Communications Privacy Act, is an attempt to react to and anticipate problems with the interception and privacy of new communications technologies.

Mr. Chairman, let me take just a few moments to highlight what I believe to be the fundamental principles which guide this legislation.

The first principle is that legislation which protects electronic communications from interceptions by either private parties or the Government should be comprehensive and not limited to particular types or techniques of communicating.

For example, it is technically impossible to effectively differentiate between wire line phone calls and those which are carried by wire, microwave, satellite, and radio. Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today—that is, cellular phones and electronic mail—is destined to be outmoded in a few years.

Now, the second principle which should be followed, I believe, in this area is a recognition that what is being protected is the sanctity and privacy of the communication. We should not attempt to discriminate for or against certain methods of communication unless there is a compelling case that all parties to the communication want the message accessible to the public.

The third principle to keep in mind is that the nature of modern recordkeeping requires that some level of privacy protection be extended to records about us which are stored outside the home.

When the Founders added fourth amendment protection against unreasonable searches and seizures to the Constitution, they did so to protect citizens' papers and effects. In those days, an individual's private writings and records were kept within the home.

That situation has changed drastically today. Many Americans are now using computer services which store their bank records, credit card data, electronic mail, and other personal data. If we fail to afford protection against governmental snooping in these files, our right of privacy will indeed evaporate.

Moreover, if we fail to protect the records of third-party providers, there will be a tremendous disincentive created against using these services. Thus, the adverse business consequence of inadequate protection for third-party records with respect to communications has led several industry groups to support—strongly support, I might add—the privacy provision of these bills.

Let me take a moment to review a bit of history. Throughout our history, there have been people who have urged us to trust the good intentions of Government officials. The logical conclusion of this approach is that we need no statutory restraints on Government investigators.

Our country's history, however, is full of instances of governmental abuse, followed by legislative or judicial response. Now, this happened with the improper interception of mail, telegraph, and telephones from the 1790's to the 1970's.

Perhaps the most important lessons from this experience are that we cannot always rely on the current policy of any single administration, and that the legislative balancing of competing interests is both more discerning and easier to adjust than ad hoc judicial determinations.

Finally, Mr. Chairman, I would like to leave with you the thoughts of Thomas Jefferson, whose comment about snooping of the post office has some currency today. He said:

> The circumstances of the times are against my writing fully and freely, whilst my own dispositions are as much against mysteries, innuendos and half-confidences. I do not know which mortifies me most, that I should fear to write what I think, or (that) my country (can) bear such a state of things.

Mr. Chairman, that concludes my statement and I thank you very much for allowing me to come here this morning.

[The prepared statement of Representative Kastenmeier follows:]

PREPARED STATEMENT OF REPRESENTATIVE ROBERT W. KASTENMEIER

Senator Mathias and Senator Leahy, it is a distinct pleasure to appear before you this morning. Each of us has spent a considerable amount of time over the past several Congresses attempting to reconcile the federal law with the challenges of new and emerging technologies. The Semiconductor Chip Protection Act exemplifies our success in the intellectual property area. The bill before you today, S. 1667, the Electronic Communications Privacy Act, is an attempt to react and anticipate problems of interception and privacy of new communications technologies. Let me take a few moments to highlight what I believe to be the fundamental principles which guide this legislation.

The first principle is that legislation which protects electronic communications from interceptions by either private parties or the government should be comprehensive, and not limited to particular types or techniques of communicating. For example, it is technically impossible to effectively differentiate between wire line phone calls, and those which are carried by wire, microwave, satellite and radio. Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today (e.g. cellular phones and electronic mail) is destined to be outmoded within a few years.

The second principle which should be followed in this area is a recognition that what is being protected is the sanctity and privacy of the communication. We should not attempt to discriminate for or against certain methods of communication, unless there is a compelling case that all parties to the communication want the message accessible to the public.

The third principle we should keep in mind is that the nature of modern recordkeeping requires that some level of privacy protection be extended to records about us which are stored outside the home. When the Founders added the Fourth Amendment's protection against unreasonable searches and seizures to the Constitution, they did so to protect citizens' papers and effects. In those days an individual's private writings and records were kept within the home. That situation has changed drastically today. Many Americans are now using computer services, which store their bank records, credit card data, electronic mail and other personal data. If we fail to afford protection against governmental snooping in these files our right of privacy will evaporate. Moreover, if we fail to protect the records of third party providers there will be a tremendous disincentive created against using these services. Thus, the adverse business consequence of inadequate protection for third-party records with respect to communications has led several industry groups to support the privacy provisions of these bills.

Let me take a moment to review a bit of history. Througnout our history there have been people who have urged us to trust the good intentions of government officials. The logical conclusion of this approach is that we need no statutory restraints on government investigators. Our country's history, however, has been full of instances of governmental abuse followed by legislative or judicial reaction. This happened with the improper interception of mail, telegraph and telephones from the 1790's to the 1970's. Perhaps the most important lessons from this experience are that we cannot always rely on the current policy of one administration, and that legislative balancing of the competing interests is both more discerning and easier to adjust than ad hoc judicial determinations.

Finally, I would like to leave you with the thoughts of Thomas Jefferson, whose comment about the snooping of the post office -- has some currency today:

> ...the circumstances of the times are against my writing fully and freely, whilst my own dispositions are as much against mysteries, innuendos and half-confidences. I do not know which mortifies me most, that I should fear to write what I think, or (that) my country (can) bear such a state of things.

That concludes my prepared statement this morning. Of course, I would be happy to answer any questions the Committee might have.

Senator **MATHIAS**. Thank you very much. Do you have time for a few questions now or would you like Mr. Moorhead to——

Mr. **KASTENMEIER**. I will wait for Mr. Moorhead, Mr. Chairman.

STATEMENT OF U.S. REPRESENTATIVE CARLOS J. MOORHEAD

Mr. **MOORHEAD**. Thank you, Mr. Chairman. It is an honor for me to be here this morning and testify in support of S. 1667, the Electronic Communications Privacy Act of 1985.

Mr. Chairman, I would like to say in the beginning that I was very sorry to hear of your announcement, because I know of the excellent job you have done as chairman of this subcommittee and of your work in the Senate. You will be sorely missed when you leave this body and we in the House will miss you, also, because you have been of great help.

Senator **MATHIAS**. Well, I appreciate those kind sentiments. I appreciate them all the more because I am not sure they are universally shared. [Laughter.]

Mr. **KASTENMEIER**. Well, if my colleague will yield, they are certainly shared by this gentleman, and I have communicated my feelings by private letter to the chairman.

Senator **MATHIAS**. You have indeed, and I appreciate both of your very kind thoughts.

Mr. **MOORHEAD**. Mr. Chairman, you and Senator Leahy, who recently presented excellent testimony before the Courts Subcommittee in the House, and Congressman Kastenmeier are to be commended for your collective efforts in developing this important legislation.

After receiving your invitation to testify, I considered several different approaches to take in regard to my testimony. I see no purpose in outlining the legislation in full again, as Congressman Kastenmeier has to some degree. I know you are aware of the contents of the legislation.

But I think it might be helpful if I detailed why I have come to support this particular approach. Several months ago, I met with representatives of the Cellular Telecommunications Industry Association.

They maintained that as technology has developed to transmit conversations over radio frequencies, as is the case with cellular, rather than through wires or cables, the applicability of title III of the 1968 Wire Tap Act has become increasingly questionable.

My initial reaction as a result of that meeting was to contemplate drafting legislation that would protect the privacy interests of cellular users. But the more I thought about it, I questioned whether or not such an approach that protected only the users of cellular would discriminate against the users of electronic mail or the users of satellite services or, for that matter, the users of any of the new electronic communications systems, and I concluded that it would.

For what is important and in need of protection is the communications themselves, for regardless of what means of communications is chosen, the expectation for privacy is still the same.

Accordingly, Mr. Chairman, I believe that any legislation that attempts to protect the privacy interests of users of the communications technology should do so in a comprehensive fashion.

S. 1667 does this by utilizing terms that deal with transmission, which is a function rather than a technology. In my opinion, legislation attempting to deal with the specifics of different technologies would be unnecessarily complex and in need of constant revision to keep pace with new innovations in this dynamic field.

Admittedly, the issues embodied in S. 1667 are complex and require a careful balancing of individual rights and law enforcement interests. Historically, when confronted with issues that have required a somewhat similar balancing of these compelling interests, I believe that Congress has proven itself equal to the task.

For example, in 1978 when Congress passed the Foreign Intelligence Surveillance Act, it struck a unique but sound balance between intelligence needs and individual rights. I would just note that I think it is a wise decision not to attempt to amend the provisions of FISA in the context of S. 1667.

Another more recent example can be found in the congressional response to the Supreme Court's decision in *Zurcher* v. *Stanford Daily*, which resulted in the Privacy Protection Act of 1980.

Mr. Chairman, I recall that you and Congressman Kastenmeier played key roles in securing passage of that legislation, which balanced the privacy interests of the press and third parties against legitimate law enforcement concerns.

I am aware, Mr. Chairman, that you and Senator Leahy and Congressman Kastenmeier have worked with the Department of Justice in drafting S. 1667, and I am sure will continue to do so.

In this regard, it is important to note that S. 1667 would enhance the interests of law enforcement by updating the provisions of Federal law relating to wiretapping and bugging. Under current law, an assistant attorney general must personally approve each interception application, while S. 1667 would permit an acting assistant attorney general to approve such applications.

The bill also expands the list of crimes for which a tap or bug order may be obtained. It would include the crimes of escape, chop shop operations, murder for hire, and violent crimes in aid of racketeering.

Again, thank you for the opportunity to testify. I look forward to working closely with you, Mr. Chairman, as well as Senator Leahy and Congressman Kastenmeier, in the days ahead toward the enactment of this legislation.

Senator **MATHIAS**. Thank you very much, Mr. Moorhead. We appreciate your being here.

Let me ask you both if you see that Senate bill 1667 or House bill 3378 would have any detrimental impact on State laws that are designed to enhance communications privacy.

Mr. **KASTENMEIER**. Mr. Chairman, if I may respond, I would say it would have no detrimental impact on State laws. It is true that some States have begun to legislate in the area. I have in mind California, which recently enacted a statute to protect cellular telephone calls.

Even more widely, many States have computer crime legislation. Since, basically, the bill, S. 1667, would amend the Wiretap Act, it would, in fact, preempt State law, as that act did originally, and would set one consistent standard.

It is also true that States would be free to enact more restrictive laws in the area if they so chose. So, to that extent, States are unaffected. But, otherwise, there would be a minimum Federal standard, obviously applicable universally in this country.

Mr. **MOORHEAD**. There is no question that some States have laws that go much farther in this direction than others, and it is very difficult to pass legislation that does not step on some toes someplace.

But I know, insofar as my own State, in particular, the problems that we are approaching with this legislation are very serious. We live in an area in California where the electronics world has come to life in all of its capabilities, and many of the radio and telecommunications people out there are concerned about the problem that this bill is trying to protect.

In the long run, I think that the laws of our State will certainly conform with the legislation that we have here, and I seriously doubt if there will be any adverse effect.

Senator **MATHIAS**. Well, I would agree with that conclusion. It does seem to me that communication is so uniquely a national function that if you were just concerned with intrastate communication, you would be limiting your protection very severely.

Now, one other question. What we are trying to do here, of course, is to respond to the new communication techniques. And as you have testified, the bill's coverage goes to the transmission and not to the technology. But do you think that we have cast a broad enough net here?

Are we likely to be outdated or rendered obsolete by new developments, or do you think we have phrased it in terms that will meet most of the challenges in the future?

Mr. **Kastenmeier**. Mr. Chairman, the original Wiretap Act is some 17 years old and obviously needs to be updated. We have attempted in your bill—I say this collectively, in S. 1667—to describe the protection in more generic terms and not in technological terms, as far as possible, this for the purpose of making the law endure the test of time and presumably comprehend new technologies as they evolve.

We cannot be sure, let us say, beyond the year 2000 or 20 years from now whether in every respect it will still be effective and not obsolete. But this is, I think, the best attempt we can make to anticipate new technologies and to make the law endure.

Mr. **Moorhead**. I think we all know that technology has been advancing so rapidly in the last decade, and I am sure that it will go even faster in the decades ahead, that we cannot anticipate everything.

But I think this legislation and the approach it takes is the one that is most likely to be able to endure because it protects the communications themselves rather than trying to outline each and every technology that could possibly be involved.

We may need some minor changes, or even major ones, in the years ahead, but I think this legislation approaches the problem as we see it today and gives us the best possible chance of a good solution.

Senator **Mathias**. Of course, this subcommittee is particularly sensitive to that because we in the Senate were not as wise and prudent as the House. You will recall that after the 1976 copyright bill we disbanded this subcommittee because we thought we had done everything that needed to be done for a generation; we thought that there would not be any need for any more legislation in this area.

We were very rapidly disabused of that thought and had to reestablish the subcommittee. So if I seem a little sensitive on that point, it is because of our errors of the past.

We are very grateful to both of you and I hope we have not held you beyond the time that it is convenient for you to be here. Thank you very much.

Mr. **Kastenmeier**. Thank you.

Mr. **Moorhead**. Thank you very much, Mr. Chairman.

Senator **Mathias**. Our next witness will be Mr. James Knapp, the Deputy Assistant Attorney General from the Criminal Division. I might say, as Mr. Knapp is taking his place, that when Attorney General Meese appeared before the Judiciary Committee at the time of his confirmation, he singled out as one of his top priorities the safeguarding of individual privacy from improper governmental intrusion.

I believe that Senate bill 1667 is the most important legislative initiative in the field of privacy to come before the Senate since the Attorney General took office. So Mr. Knapp's testimony is particularly welcome. His statements on behalf of the Department of Justice will be important.

Before you testify, Mr. Knapp, I see that Senator Leahy has arrived. Let me ask if he has a statement.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator **Leahy**. Thank you, Mr. Chairman; I do, and I am sorry to have missed Representative Kastenmeier, who has worked so hard in this area over in the House. Unfortunately, like all of us, I had other things going on. Something started at 8, which was supposed to be through by 9, and dragged on forever.

I would like to put a statement in the record, but I wonder if I might just go through the first page, because there are some items that I would like the Justice Department to hear.

I would like to describe three scenes, each of which is probably going on somewhere right now somewhere in the United States. The first involves two business people who are discussing their company's financial data over the telephone. Unknown to them, a member of a competitor company is listening in on their conversation by means of a phone tap.

The second involves a police officer who has a hunch that Jane Doe is involved in drug trafficking. The officer goes to the post office and tells the postal clerk that he wants to open and read Ms. Doe's mail and then have it resealed and delivered.

The third scene involves a man who, goaded by TV advertising, decides to reach out and touch somebody. He picks up his telephone and calls his old college roommate The roommate's next-door neighbor listens in on their conversation with a phone tap.

Now, no one here would disagree that each of the eavesdroppers' conduct in these examples is wrong. It is also illegal. Let me change the examples.

In the first case, instead of the two business people discussing financial matters over the telephone, they use a video teleconference system which displays their proprietary data on their video screens. The same data is picked up by their competitor.

In the second case, the police officer goes to an electronic mail company, not the post office. Ms. Doe is a user of the system and the officer asks to see all of her messages.

In the third case, rather than speaking on the telephone, the man uses a computer keyboard to type a message to his former roommate. The message is intercepted by the neighbor on his own computer system.

I think everyone here would still agree that the conduct of these electronic eavesdroppers is wrong. What is not at all clear in the law today is whether it is also illegal, and that is the question we really raise by this.

This electronic mail, this electronic data transfer, electronic communication—should the eavesdropping of that be illegal in the same way that we have made illegal the well-known wiretap on somebody's telephone?

So I will, by unanimous consent, if the chairman has no objection, put the rest of my statement, which is equally brilliant, entertaining and exciting, into the record. I do that for two reasons. One, because I wanted it printed and, second, because the chairman has had to listen to the same speech so many times before.

How is that?

Senator **Mathias**. In view of the fact that I have made the same sacrifice and have deprived this audience of the same kind of wisdom, I have no objection.

[Senator Leahy's prepared statement follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

Mr. Chairman. I would like to begin the hearing today by describing three scenes, each of which is probably going on somewhere right now.

The first involves two business people who are discussing their company's financial data over the telephone. Unknown to them, a member of a competitor company is listening in on their conversation by means of a phone tap.

The second involves a police officer who has a hunch that Jane Doe is involved in drug trafficking. He goes to the post office and tells the postal clerk that he wants to open and read Ms. Doe's mail, and then have it resealed and delivered.

The third scene involves a man who, goaded by TV advertising, decides to reach out and touch someone. He picks up his telephone and calls his old college roommate. The roommate's next door neighbor listens in on their conversation with a phone tap.

No one here would disagree that each of the eavesdroppers' conduct in these examples is wrong. It is also illegal.

Now let me change my examples.

In the first case, instead of the two business people discussing financial matters over the telephone, they use a video teleconference system which displays their proprietary data on their video screens. The same data is picked up by their competitor.

In the second case, the police officer goes to an electronic mail company. Ms. Doe is a user of the system and the officer asks to see all of Ms. Doe's messages.

In the third case, rather than speaking on the telephone, the man uses a computer keyboard to type a message to his former roommate. The message is intercepted by the neighbor on her own computer system.

I think everyone here would still agree that the conduct of these electronic eavesdroppers is wrong. What is not clear is that it is also illegal.

Not long ago, a message was transmitted by first class mail, by wire, or by some form of wireless communications link. Each had its advantages and vulnerabilities. Each was regulated by separate legislation that provided a legal framework of appropriate privacy protection of the user. It was a neat and tidy world, in which private users, common carriers, and government each knew their rights and limits.

But the technological changes of the last decade have left the privacy protection afforded to individual Americans and American businesses in tatters.

When Congress enacted the federal wiretap law in 1968, it had in mind a particular kind of communication--voice--and a particular way of transmitting that communication--via a common carrier analog telephone network. Congress chose to cover only the "aural acquisition" of the contents of a common carrier wire communication. The Supreme Court has interpreted that language to mean that to be covered by Title III, a communication must be capable of being overheard.

Thus, there is no adequate legal protection against the unauthorized interception of data transmissions.

There is no adequate legal protection against the unauthorized interception of communications in private, non-common carrier networks.

There is no adequate federal legal protection against the unauthorized access of electronic communications system computers to obtain or alter the communications contained in those computers.

There is no adequate legal protection afforded to cellular radio telephones, electronic pagers and the private transmissions of video signals such as that used in teleconferencing.

S. 1667, introduced by Senator Mathias and myself, and an identical bill, H.R. 3378, introduced in the House by Congressmen Kastenmeier and Moorhead, are aimed at all those problems. This legislation will go a long way towards providing the legal protections of privacy and security which are necessary to insure the continued growth of new communications technologies.

The Electronic Communications Privacy Act contains five important changes to the current federal wiretap law.

First, it will extend the coverage of the law from only voice transmissions to all electronic communications. It will cover the transmission of digitized data by telephone, or the transmission of video images by microwave, or any other conceivable mix of medium and message.

Second, the bill recognizes that private carriers and common carriers perform so many of the same functions today that the distinction no longer serves to justify different privacy standards. All systems designed to carry private messages will be covered.

Third, the bill will create civil and criminal penalties for the unauthorized access to the computers of an electronic communication system, if information is obtained or altered. It does little good to prohibit the interception of information while it is being transmitted, if similar protection is not afforded to the information while it is being stored for later forwarding.

Fourth, civil remedies are provided for the unauthorized disclosure of the contents of a particular electronic message which results in harm to the parties to the communication.

Finally, the bill provides that a law enforcement agency must obtain a court order under appropriate standards before it is permitted access to the records of an electronic communication system. This requirement, while protecting the government's legitimate law enforcement needs, will minimize intrusiveness for both system users and service providers. It will also give users the right to contest unlawful government actions.

Mr. Chairman, we have worked hard over the past year to listen to all affected interests and to accommodate the legitimate needs of law enforcement while securing the privacy rights of users and operators of electronic communications systems.

Most reactions have been very favorable, but some difficult questions remain to be answered.

We are fortunate to have some distinguished witnesses here today who have come with specific concerns and suggestions of how the bill can be strengthened.

I look forward to their testimony.

Senator **Mathias**. Mr. Knapp.

STATEMENTS OF JAMES KNAPP, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, ACCOMPANIED BY HARRY MYERS, ASSOCIATE CHIEF COUNSEL, DRUG ENFORCEMENT ADMINISTRATION; AND FREDERICK HESS, DIRECTOR, OFFICE OF ENFORCEMENT OPERATIONS, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. **Knapp**. Thank you, Mr. Chairman, Senator Leahy. It is a great pleasure to be here this morning to testify before you on this important subject.

Seated with me this morning to help answer technical questions, to my right, is Harry Myers, the associate chief counsel of the Drug Enforcement Administration. To my left is Frederick Hess, the director of the Office of Enforcement Operations in the Criminal Division, which is responsible for processing title III requests in the Department.

I am going to offer for the record my prepared statement, which I will summarize so as to leave time for questioning. I would, however, like to make a correction.

On page 5 of the testimony, there is a reference, in the middle of the page, to digital transmissions. The title is set out separate and apart from the title to subpart A. That is a mistake. It should be part of the title to subpart A, with a semicolon thereafter.

S. 1667, the Electronic Communications Privacy Act of 1985, is directed primarily at amending title III of the Omnibus Crime Control and Safe Streets Act of 1968 to provide coverage of new technologies that were not available when the original act was passed in 1968.

In addition, the bill provides for more comprehensive judicial supervision of investigative methods related to electronic surveillance that are not now within the scope of title III.

Initially, I would note that title III electronic surveillance is an extremely valuable and effective law enforcement tool. I would direct your attention to my prepared testimony, which discusses specifically a survey which is in progress right now in the Justice Department.

We took a random sample of 51 cases from fiscal year 1983 in which wiretaps were authorized; 45 of those 51 cases have resulted in one or more indictments in each investigation, which is a very high percentage for any particular type of investigative tool. And most of those indictments have already resulted in a large number of convictions

I would also stress that there is no record of abuse of electronic surveillance under title III and that the rate of suppression of evidence obtained by means of electronic surveillance for any reason is miniscule.

As this committee knows, the current laws governing interception of communications are complex and attempt to strike a balance between legitimate privacy concerns and the responsibility of Federal officials to arrest and prosecute criminals.

While we in the Department of Justice are mindful of the privacy rights of our citizens, we think it is equally necessary to recognize the importance of court-ordered interceptions of communications in investigating major crimes.

Title III has succeeded in providing an appropriate balance between the citizen's right to privacy and the law enforcement and societal interests in preventing crime and apprehending criminals.

The statute has proven itself amenable to application to a number of new technologies, although certainly not to all that have been developed. In addition, since the enactment of title III, a substantial body of case law has developed which establishes well-defined limits on how the statute is to be used and how it is to be interpreted.

Relative to any assessment of the statute in terms of proposed amendments to address technological developments, care must be taken not to impair this existing and well-understood statutory structure.

Before bringing certain investigative aids under judicial supervision, great care must be taken to balance new impediments to important investigative techniques against the degree of intrusion actually involved.

Judicial supervision is required when the degree of intrusion is such that it infringes upon an individual's reasonable expectation of privacy. The Department does agree that the electronic surveillance provisions of title III should be reevaluated periodically to ensure that the statute keeps pace with developing technology.

We recognize that certain modifications, due to the rapidly changing technology of electronic communication, may be necessary, and we feel that some of the amendments proposed in S. 1667 address this need.

However, we have serious concerns about many of those provisions of this bill which could unnecessarily complicate procedures without significantly enhancing individual rights of privacy, or without enhancing privacy rights in any meaningful way.

We would stress that a great deal of further analysis and discussion is required before the implications of the new technologies are fully understood.

Let me briefly discuss the applicability of the proposed bill to the following specific technological advances. First, cellular and cordless telephones; we believe all forms of conventional telephones, as well as many of the newer technologies, are currently covered by title III because the transmission is at least in part by wire.

There may be a need to amend the statute to specifically cover those types of telephones where the communication is transmitted by means of radio. My statement raises a number of questions that must be looked at carefully before any definitive recommendations can be made in this area.

Second, computer transmissions and electronic mail are covered by the ordinary search warrant process, based on probable cause pursuant to rule 41 of the Federal Rules of Criminal Procedure.

Electronic mail is entitled to no greater protection than regular mail. Consequently, we do not believe it should be brought under the scope of title III.

Third, video surveillance; under present case law the Government would secure an order under rule 41 of the Federal Rules of Criminal Procedure where there is only video surveillance, assuming the video surveillance involves a reasonable expectation of privacy. If there is to be any audio interception, a separate title III authorization is procured.

Under this procedure, individual rights are adequately safeguarded. Adding video surveillance by itself to title III would be adding an entire new scope to the statute. There is no need for that at this time since most instances of video surveillance do not involve areas where there is a reasonable expectation of privacy.

The bill also contains provisions in the areas involving investigative techniques somewhat related to title III, but not presently within the coverage of the statute. The thrust of these provisions is to take investigative techniques that do not approach the level of intrusion involved in the actual interception of the contents of communications accomplished by full-scale electronic surveillance and elevate them virtually to the same level.

The result would be a severe hindrance to law enforcement in using nonintrusive techniques to combat drug trafficking, organized crime, and terrorism. First, let me discuss paging devices.

There are presently three types of such devices. The first type, the tone pager, only transmits a beeping sound to the handset carried by the subscriber. No message of any type is transmitted and it is the Department's position that interception of the beep does not constitute a search and should not be regulated under the statute.

The second type, the digital beeper, transmits digitized numbers and arguably a message could be transmitted by using these numbers. The present practice is to procure an order under rule 41 of the Federal Rules of Criminal Procedure to intercept this type of communication.

The third type of paging device, the voice page, transmits an aural message, and present practice is to secure an interception order under title III before this type of message is intercepted.

We have no objection to the codifying existing standards, but we would object to increased levels of supervision.

Second, pen registers; S. 1667 would amend title 18 to add a new chapter bringing the use of pen registers and tracking devices under increased judicial supervision. It is the Department's position that this change would create serious problems for law enforcement.

It is currently the practice of the Department to secure court orders——

Senator MATHIAS. Mr. Knapp, I am sorry to interrupt you, but there is a rollcall vote in progress in the Senate. So I am afraid we will have to take a 5-minute recess. Senator Leahy can jog there and back in 5 minutes.

Senator LEAHY. Are you going, too?

Senator MATHIAS. Yes.

Senator LEAHY. I will jog along with you.

Senator MATHIAS. We will resume as soon as we get back.

[A brief recess was taken.]

Senator MATHIAS. Mr. Knapp, did you want to say anything further?

Mr. **Knapp**. Yes, I do. I left off on pen registers and then I will discuss some of the examples that Senator Leahy posed, if you would like me to.

Senator **Mathias**. All right. If you can bring your testimony to a close as quickly as possible, then we can get on to questions, because there will be some serious questions.

Mr. **Knapp**. I was discussing pen registers and I pointed out that it is currently the Department's practice to secure court orders pursuant to rule 57 of the Federal Rules of Criminal Procedures, upon a representation to the court that the pen register information is relevant to an ongoing criminal investigation.

Increasing judicial supervision would severely limit the effectiveness of pen registers and their utility to law enforcement. We would oppose any change or special provisions for pen registers.

Similarly, I discuss in my testimony the problem of toll records and location tracking devices. I think that is fairly clearly set forth.

We do have some affirmative recommendations which are discussed in more detail in my prepared statement. I would like to call your attention specifically to the provision enabling us to utilize nonagent personnel to monitor some of these wire interceptions. Such a change would be of tremendous practical assistance to the agencies involved, assuming appropriate training and supervision can be provided.

There are also some other affirmative recommendations that we would like to call to your attention.

Taking the three examples which Senator Leahy mentioned, there may be some misunderstanding here. In the first case, he says two business people are discussing financial matters over the telephone. They use a video teleconference system which displays their proprietary data on video screens. The same data is picked up by their competitor.

I assume from the hypothetical that there is no audio involved. If that is the case, title III would not apply, but clearly a search warrant would be required for Government agencies.

However, there is apparently nothing right now that would cover interception by private individuals. We have no objection to such legislation, but we do not believe that it should be part of title III.

The second situation, electronic mail, that is clearly covered by the search warrant process. And as I emphasized in my statement, we do not believe that electronic mail should be treated any differently than private mail is now treated.

In the third situation, rather than speaking on a telephone, a man uses a computer keyboard to type a message to his former roommate. The message is intercepted by the neighbor on her own computer system.

As with the first hypothetical, to the extent that this involves activity by private individuals, it is something which could be dealt with by separate legislation. We do not feel that title III is the appropriate vehicle for doing so because that would seriously add unnecessarily to law enforcement procedures.

The search warrant process is adequate for law enforcement, and therefore to the extent that conduct by private citizens needs to be regulated, that should be done by separate legislation.

I want to restate once again, as you pointed out, that Attorney General Meese clearly wants to ensure the protection of privacy of individual citizens in this country. This is a top priority of his, but we want to do so in the most effective way.

Title III is not always the most appropriate vehicle to do so; it is for some technologies, not for others. The traditional search warrant requirements for the Government or special legislation for eavesdropping by private individuals may be the most appropriate, depending on the technology involved.

With those general comments, Senator, I will be glad to answer any questions you have.

[Mr. Knapp's prepared statement follows:]

PREPARED STATEMENT OF JAMES KNAPP

Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to appear here today to discuss S.1667, the Electronic Communications Privacy Act of 1985.

The proposed legislation is directed primarily at amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to provide coverage of new technologies in the area of communications and electronic surveillance that were not available when the original act was passed in 1968. In addition, the proposed legislation provides for more comprehensive judicial supervision of investigative methods related to electronic surveillance heretofore not within the scope of Title III.

We have serious concerns about many of those provisions of this bill which could unnecessarily complicate procedures without enhancing individual rights of privacy.

An in depth review of the proposed legislation is presently being conducted by several Department of Justice components whose activities would be affected by this bill. Because of the complexity of this type of legislation that analysis has not yet been completed. The President's Commission on Organized Crime is also in the process of evaluating the effectiveness of Title III and it is my understanding that the Commission will be making recommendations relative to the effectiveness of the statute in the near future. So rather than addressing the specific language of the bill, I will limit myself to making a number of general comments and observations about certain proposals in the legislation, and then identifying some particular problems which we feel ought to be addressed.

Initially, I would note that Title III electronic surveillance is an extremely valuable and effective law enforcement tool. Its value was proved recently by a survey taken by the Criminal Division's Office of Enforcement Operations to test the results of court ordered electronic surveillance in 1983. That year was chosen to give sufficient time for investigations to be completed and most trials to be over. We chose, at random, 51 investigations which, with related wiretap authorizations, covered 35% of the total of new Title III authorizations for that year. All reports are still not complete, but our figures indicate that convictions, indictments and ongoing investigations in which indictments are expected have occurred in 45 of the 51 investigations; which is a rate of 88%. In addition, in just 38 completed investigations, convictions of those originally named as interceptees or others later found to have been involved in the investigation total 467 or an average of almost 13 convictions per completed investigation. Currently another 64 individuals are under indictment in the remainder of the open investigations and a good number of further indictments are expected in those investigations that still have not reached the indictment stage.

We believe these figures, which we continue to amass and analyze, show the great effectiveness of Title III as a law enforcement tool. We must also stress that there is no record of abuse of electronic surveillance and that the rate of suppression of evidence obtained by means of electronic surveillance for any reason is minuscule.

As you know, the current laws governing interception of communications are complex and attempt to strike a balance between legitimate privacy concerns and the responsibility of federal officials to arrest and prosecute criminals. While we in the Department of Justice are mindful of the privacy rights of our citizens, we think it is equally necessary to recognize the importance of court-ordered interceptions of communications in investigating major crimes. In the Department's judgment, Title III of the Omnibus Crime Control and Safe Streets Act has succeeded in providing an appropriate balance between the citizen's right to privacy and the law enforcement and societal interest in preventing crime and apprehending criminals. The statute has proven itself amenable to application to a number of new technologies although certainly not to all that have been developed. In addition, since the enactment of the statute in 1968, a substantial body of case law has developed which establishes well defined limits on how the statute is to be used and how it is to be interpreted. Relative to any assessment of the statute in terms of proposed amendments to address technological developments, care must be taken not to impair this existing and by now well understood statutory structure.

Moreover, before bringing certain investigative aids under judicial supervision, as the proposed bill does, great care must be taken to balance new impediments to important and well established investigative techniques against the degree of intrusion involved. In our view, judicial supervision is required when the degree of intrusion is such that it infringes upon an individual's reasonable expectation of privacy. This, of course, is the principle embodied in Title III and in the Supreme Court's decisions interpreting the Fourth Amendment.

I. NEW TECHNOLOGIES

The Department of Justice does agree that the electronic surveillance provisions of Title III should be re-evaluated periodically to ensure that the statute keeps pace with developing technology. Our policy is to propose amendments to the statute and to support those amendments proposed in Congress whenever our experience and continuing review of the statute warrant such action. At the present time, we recognize that certain modifications due to the rapidly changing technology of electronic communication may be necessary and we feel that some of the amendments proposed in S.1667 address this need. We would stress, however, that a great deal of further analysis and discussion is required before the implications of the new technology are fully understood.

DIGITAL TRANSMISSIONS

A. CELLULAR AND CORDLESS TELEPHONES

Although the Department believes that all forms of conventional telephones as well as many of the newer technologies are currently covered by Title III because the transmission is at least in part by wire, there may be a need to amend the statute to specifically cover those types of telephones, like cellular telephones and certain forms of cordless telephones, where the communication is transmitted partly by means of radio. The radio portion of the transmission is either analog (regular voice transmission), digitized, or encrypted in some other fashion. The analog transmission would readily be subject to interception by an ordinary citizen with a standard AM/FM radio receiver by tuning to certain frequencies. Digitized or otherwise encrypted transmissions would require specialized equipment to turn the conversation back into analog form. In amending the statute to cover these new forms of telephones, a decision has to be made as to whether all communications should be covered including analog conversations when transmitted as radio communications. If so, would an ordinary citizen who intercepts them be subject to criminal or civil liability? Should there be a reasonable expectation of privacy where such calls are so suspectible to interception? In the alternative, should amendments to the statute respecting these types of telephones only be extended to the radio portions of the communications that are digitized or encrypted in some other manner where additional technical steps must be taken to turn the digitized communication back into analog form so it could be understood?

The Department has not yet formulated a policy on whether only a digitized or otherwise encrypted conversation should be subject to the protection of the statute. It could be argued that the additional protection for the call by digitizing or otherwise encrypting it would evince a clear intent that there is a reasonable expectation of privacy. In this scenario, the citizen who either voluntarily or involuntarily intercepts the analog call would be free of criminal or civil liability. Obviously, so too should law enforcement personnel. These are questions that have to be looked at carefully before definitive recommendations can be made.

B. COMPUTER TRANSMISSIONS AND ELECTRONIC MAIL

Second, with respect to the legislation's attempt to bring within the proscriptions of Title III the newer types of non-aural transmissions such as computer transmissions and electronic mail, it is our current belief that with respect to authorization for the government to seize the contents of these transmissions, they are covered by an ordinary search warrant process based on probable cause pursuant to Rule 41 of the Federal Rules of Criminal Procedure. For example, if the government presently wishes to intercept a letter posted with the Postal Service, a search warrant under Rule 41 is procured. The Department believes that electronic mail is entitled to no greater protection than regular mail. Including these transmissions in Title III would, in effect, be adding an entire new scope to the existing statute. Had Congress intended that in 1968, it would have added non-aural communications such as ordinary mail in the statute at that time. The Department feels that changing the entire thrust of Title III is not warranted at this time and that intercepting this type of non-aural communication by private individuals could better be handled by separate legislation. The safeguards regulating government interception at this time are adequately covered by Rule 41 of the Federal Rules of Criminal Procedure. A similar analysis appears appropriate for computer transmissions.

C. VIDEO SURVEILLANCE

Video surveillance is a relatively new investigative tool. Two different types of situations must be considered when trying to legislate controls over this technology. The first is the situation where the government is conducting video surveillance of an individual or a premises where there is a reasonable expectation of privacy. The second type of video surveillance is where a closed circuit video transmission is intercepted by either the government or an individual.

The most common type of situation that arises with respect to government activity is the surveillance of an individual or a premises where there is a reasonable expectation of privacy. Under present case law, the government would secure an order in the nature of a search warrant under Rule 41 of the Federal Rules of Criminal Procedure where there is only video surveillance, assuming the video surveillance involves a reasonable expectation of privacy. If there is to be any audio interception then a separate Title III authorization is procured. Under this procedure the rights of the citizen are adequately safeguarded. Adding video surveillance by itself to Title III would again be adding an entire new scope to the statute. The Department sees no need for that at this time particularly since most instances of video surveillance do not involve areas where there is a reasonable expectation of privacy. We would have no objection to authorizing courts to approve a continued video and audio surveillance in a single Title III order.

Considering the scenario where a closed circuit television transmission between two individuals would be intercepted, it is highly unlikely that such a transmission would take place without an audio portion relaying information on the image. Where the audio transmission is present, Title III adequately covers the communication. Interception of the video portion alone by government agents would be covered by Rule 41 so the only difficulty arises where the video transmission (with no audio accompanist) is intercepted by someone other than a law enforcement officer. This very rare situation could be covered in the same type of legislation that would regulate computer hacking without disturbing the purpose and intent of Title III.

II. INVESTIGATIVE TECHNIQUES

With respect to S.1667, the Department has serious objections to several of the bill's other provisions in the areas involving those investigative techniques somewhat related to Title III but not presently within the coverage of that statute. The thrust of these provisions is to take investigative techniques that do not approach the level of intrusion involved in the actual interception of the contents of communications accomplished by full scale electronic surveillance and elevate them virtually to the same level. The result will be a severe hindrance to law enforcement in using non-intrusive techniques to combat drug trafficking, organized crime, and terrorism.

A. PAGING DEVICES

Although not specifically delineated in the proposed legislation, the new definitions would include paging devices under the proscriptions of the revised Title III.

There are presently three types of such devices. The first type, the tone pager, only transmits a beeping sound to the handset carried by the subscriber. No message of any type is transmitted and it is the Department's position that interception of the beep does not constitute a search and should not be regulated under the statute. The second type, the digital beeper, transmits digitized numbers and arguably a "message" could be transmitted by using numbers. Present practice is to procure an order under Rule 41 of the Federal Rules of Criminal Procedure based on probable cause to intercept this type of communication. Since no aural message is transmitted, it is the Department's position that Title III does not presently apply to this type of paging device. The third type of paging device, the voice pager, does in fact transmit an aural message and present practice is to secure an interception order under Title III before this type of message is intercepted.

It is the Department's position that present standards balance the rights of the individual with the interests of law enforcement and that new legislation should not escalate the levels of judicial supervision for the utilization of these devices over present standards. The third type of paging device should appropriately remain under Title III, while the second type should continue to be regulated by Rule 41 of the Federal Rules of Criminal Procedure. The first type which transmits a beep only should not be subject to judicial supervision because of the de minimus level of intrusion.

The Department has no objection to codifying existing standards but would object to increased levels of supervision as imposing an undue burden on the use of the devices by law enforcement agents.

B. PEN REGISTERS

S.1667 would amend Title 18 of the United States Code to add a new chapter bringing the use of pen registers and location detection devices (tracking devices) under increased judicial supervision. It is the Department's position that this change would create serious problems in the law enforcement procedures that have developed under Title III.

Pen registers are attached to telephones only for the purpose of identifying and recording dialed numbers. Their use does not infringe on any constitutionally protected interest and that has clearly and definitively been decided by the Supreme Court. Smith v. Maryland, 442 U.S. 735 (1979). Pen registers have proven to be a valuable tool in criminal investigations, especially those involving drug trafficking, organized crime activities, and money laundering where perpetrators frequently use the telephone to communicate. The pen register enables the investigators to establish a pattern of communication between suspects. It never permits access to the contents of a conversation. It is currently the practice of the Department to secure court orders authorizing the use of pen registers pursuant to Rule 57 of the Federal Rules of Criminal Procedure. Assistant United States Attorneys in the field may secure these orders, without the review of senior Department officials, upon a representation to the court that such information is relevant to an ongoing criminal investigation. Inasmuch as this procedure does not require a showing of "probable cause" to obtain the order, pen registers have proven especially effective at the earlier stages of investigations when the primary objectives are identifying the participants and determining their relationship in the alleged criminal activity. In many instances, the results of the pen registers are then used to develop the more detailed showing of "probable cause" necessary to obtain Title III orders authorizing the far more intrusive interception of wire and oral communications.

The proposed bill at page 16 establishes a standard of reasonable cause to believe that the information likely to be obtained by such installation and use is relevant to a legitimate criminal investigation before a pen register can be authorized. The Department objects to this language. It escalates the level of judicial review in a manner inappropriate to the degree of intrusion on privacy interests that pen registers cause. If the assistant United States Attorney makes a representation to the court that a pen register is relevant to a criminal investigation, that should be sufficient and more should not be required. The difference between "reasonable" and "probable" cause is not readily discernible and this ambiguity would, we think, result in too great a degree of proof.

Bringing the use of pen registers within increased judicial supervision would limit their use and would impose many of Title III's elaborate procedures. Consequently, the use of pen registers would significantly decline to the detriment of criminal investigations and ultimately the prosecutions themselves. Given that pen registers, by comparison to the interception of communications, constitute a minimal intrusion into the privacy interests of targeted subjects, it is the Department's view that it is unnecessary and inappropriate to increase judicial supervision over their use.

Given that no communications are intercepted and that the courts have held that there is no constitutional or statutory requirement for court supervision of a pen register, the bill's elaborate notification and reporting requirements would create an unnecessary burden on law enforcement resources that would not be balanced by an equal benefit to citizen rights of privacy.

C. LOCATION DETECTION DEVICES (TRACKING DEVICES)

Similarly, to include location detection devices (tracking devices) under Title III would have an adverse impact on law enforcement efforts. In most instances the use of location detection devices (tracking devices) like pen registers, invades no constitutionally protected interests. See e.g., United States v. Knotts, 460 U.S. 276 (1983). Such devices never reveal the content of any conversation. In those cases in which the installation or monitoring of location detection devices (tracking devices) would invade a subject's reasonable expectation of privacy, e.g., United States v. Karo, 104 S. Ct. 3296 (1984), court orders pursuant to a showing of "probable cause" are sought under Rule 41 of the Federal Rules of Criminal Procedure. In these instances as well, however, review and approval of the applications by senior Department officials is not required.

Like pen registers, location detection devices (tracking devices) have proven to be an effective and often vital investigative tool, especially in drug investigations where they are used to track shipments of contraband and vehicles that transport those shipments. Their use often eliminates the need to commit substantial resources required for "moving" physical surveillance. The practical effect of subjecting the use of location detection devices (tracking devices) to increased judicial and administrative supervision would be to narrow severely the circumstances in which they could be effectively utilized. Because location detection devices (tracking devices) like pen registers very rarely involve any infringement into the privacy interests of the subject, it is unnecessary to impose upon their use the stringent controls and reporting requirements.

In addition, the reporting requirements imposed by the legislation would cause serious difficulties in the utilization of these procedures. The Department feels that the minimal levels of intrusion involved in using these devices does not warrant significant reporting requirements.

D. TOLL RECORDS

The proposed bill has a provision that would add to Title 18 a new subsection 2511(4), which would require a court order for the government to obtain telephone toll records. Telephone toll records, like pen registers, never reveal the contents of a conversation and invade no reasonable expectation of privacy. Even if the criteria required for securing the order under the bill -- reasonable suspicion that a person or entity by whom or to whom the communications were made has engaged, or is about to engage, in criminal conduct and that the records may contain information relevant to the conduct -- does not rise to the probable cause level required for securing an eavesdropping court order, the requirement nevertheless does impose a heavy procedural burden on law enforcement officials in an area that is minimally intrusive and has proven to be a highly effective law enforcement tool. It is the view of the Department of Justice that present procedures for securing this information by either an administrative subpoena from a law enforcement agency with such power or by way of a grand jury subpoena provide sufficient safeguards against the abuse of this process.

E. ADDITIONAL PROCEDURAL REQUIREMENTS

The additional requirements imposed by the proposed legislation relative to providing further specific information in the applications and the orders on a) investigative objectives and b) alternate investigative techniques are unnecessary and would be more burdensome. The statute and the case law that has developed clearly defines the parameters of what is necessary to obtain the order. The law is clear that electronic surveillance need not be the only remaining alternative as long as the court is satisfied that the other investigative methods are likely not to succeed or would be too dangerous. That showing must now be made before an order is issued.

The Department would oppose the proposed amendment to 18 U.S.C. 2518 (8)(a) that would change the wording of that portion of the statute which mandates presenting the recording tapes of the intercepted conversations to the judge "immediately" upon the expiration of the authorization to presenting the tape recordings "not later than 48 hours", courts have clearly held that they should be presented as soon as possible but that, for good cause shown, courts can excuse delays depending upon the situation. Current case law has given this discretion to the judge and legislating a specific time would be too limiting in practice and would require re-interpretation by the courts. Nor is there any practical reason to mandate ten day reviews by courts of the status of individual wiretaps. Courts are presently able to impose such requirements, where warranted at appropriate intervals.

Finally, we wish to draw attention to the changes in the proposed level of culpability of a violator in both the criminal and civil areas. Section 2520 of Title 18 currently provides that a good faith reliance on a court order or legislative authorization is a complete defense to both civil and criminal actions brought under Title III or any other law. Section 103 of the proposed legislation, which is intended to replace Section 2520 of the current statute, provides that a good faith reliance on a court order or warrant is a complete defense to only a civil action. Thus, the implications of the proposed legislation are unclear as to the level of criminal liability of an agent who in the course of his or her duties inadvertently violates the law. To impose a criminal liability for what would at most be ordinary negligence is exceedingly harsh and would inhibit those involved in conducting legitimate investigations. The Department would like to see a good faith exception to both criminal and civil liability as well as a good faith exception to the exclusionary rule for presentation of evidence under appropriate circumstances.

III. AFFIRMATIVE RECOMMENDATIONS

The Department in its experience with the provisions of Title III has identified certain areas where affirmative amendments would greatly facilitate the law enforcement function.

The first of these areas is the extension of Title III authorization authority to interceptions of specified individuals wherever they may be as well as to places and facilities in line with the theory of Katz v. U.S. 389 U.S. 347, that the Fourth Amendment protects people not places. We realize this suggestion raises interesting and novel issues of a constitutional nature. We raise it to stimulate debate at this time in the hope that an appropriate vehicle can be drafted to permit this form of authorization.

We also recommend extending Title III authorization to cases involving bail jumping where the underlying offenses would have supported a Title III request and to prison escapes. We support the addition of the new offenses in Section 105 of the proposed legislation and would recommend adding air piracy and hostage taking to those offenses.

The Department favors the proposed provision of the bill that would authorize an Acting Assistant Attorney General in charge of the Criminal Division to sign Title III authorizations.

The Department endorses the proposed legislation's provisions that would authorize the use of mobile interception devices (p. 11 of the statute) and tracking devices (p. 16 of the statute) across district lines where the order is procured in the district of origin.

An amended statute should have a provision that the 30-day authorization period for a Title III should begin to run upon installation of the interception device and not on signing of the order.

The Department also favors expanding the category of people who can help monitor the interception of communications, such as clerical personnel in the enforcement agencies.

In conclusion, new technologies may warrant a re-examination of the scope and adequacy of existing Title III provisions now available. We feel that some additional study and review should be considered. Consideration should also be given to the changes that the Department has suggested. These changes listed are not exhaustive of those changes that might facilitate effective and proper use of Title III, but they are illustrative of practical problems which could be solved by new legislation. We would be pleased to work with the Subcommittee's staff in developing a bill that all can support.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions at this time.

Senator **Mathias**. The Office of Technology Assessment has recently completed a thorough study of the topic "Electronic Surveillance and Civil Liberties." OTA concluded that the law has not kept pace with the technological changes in the communications field and outlined several options for congressional action.

It seems to me that this might be an appropriate point to include the summary of the report, contained in chapter 1 of that report. The whole report is, I think, too large a document to include in the record of this hearing today, but to place a summary in the record in conjunction with the Department of Justice's comments would be useful.

[The following excerpt was submitted for the record:]

[EXCERPT]

Federal Government Information Technology

Electronic Surveillance and Civil Liberties

OTA Reports are the principal documentation of formal assessment projects. These projects are approved in advance by the Technology Assessment Board. At the conclusion of a project, the Board has the opportunity to review the report, but its release does not necessarily imply endorsement of the results by the Board or its individual members.

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D.C. 20510

Chapter 1

Summary

In the last 20 years, there has been a virtual revolution in the technology relevant to electronic surveillance. Advances in electronics, semiconductors, computers, imaging, data bases, and related technologies have greatly increased the technical options for surveillance activities. Closed circuit television, electronic beepers and sensors, and advanced pen registers are being used to monitor many aspects of individual behavior. Additionally, new electronic technologies in use by individuals, such as cordless phones, electronic mail, and pagers, can be easily monitored for investigative, competitive, or personal reasons.

The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance applications. The fourth amendment—which protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures"—was written at a time when people conducted their affairs in a simple, direct, and personalized fashion. Telephones, credit cards, computers, and cameras did not exist. Although the principle of the fourth amendment is timeless, its application has not kept abreast of current technologies.

The major public law addressing electronic surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which was designed to protect the privacy of wire and oral communications. At the time Congress passed this act, electronic surveillance was limited primarily to simple telephone taps and concealed microphones (bugs). Since then, the basic communications infrastructure in the United States has been in rapid technological change. For example, satellite communication systems and digital switching and transmission technology are becoming pervasive, along with other easily intercepted technical applications such as cellular mobile radio, cordless telephones, electronic mail, computer conferencing, and electronic bulletin boards. Continued advances in computer-communications technology such as the Integrated Services Digital Network (ISDN), now close to implementation, are likely to present additional new opportunities for electronic surveillance.[1]

The law has not kept pace with these technological changes. The courts have, on several occasions, asked Congress to give guidance. Most recently, U.S. Circuit Court Judge Richard Posner, in a case involving the use of video surveillance in a law enforcement investigation, said:

> . . . we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope . . . judges are not authorized to amend statutes even to bring them up to date.

In legislating the appropriate uses of electronic surveillance, Congress attempts to strike a balance between civil liberties—especially those embodied in the first, fourth, and fifth amendments to the U.S. Constitution—and the needs of domestic law enforcement and investigative authorities for electronic surveillance in fighting crime, particularly white-collar and organized crime, and generally for drug, gambling, and racketeering investigations.[2]

Law enforcement and investigative agencies, at least at the Federal level, are making significant use of electronic surveillance techniques and are planning to use many new techniques. Based on a review of available reports and the results of its Federal Agency Data Request,[3] OTA found that:

---

[1] ISDN permits the transmission of voice, video, and data signals as needed over a common multi-purpose communications network.

[2] Note: This study did not review technology or policy issues concerning foreign intelligence and counterintelligence applications of electronic surveillance.

- The number of Federal court-approved bugs and wiretaps in 1984 was the highest ever.
- About 25 percent of Federal agency components responding (35 out of 142) indicated some current and or planned use of various electronic surveillance technologies, including, but not limited to, the following:
  - —closed circuit television (29 agencies);
  - —night vision systems (22);
  - —miniature transmitters (21);
  - —electronic beepers and sensors (15);
  - —telephone taps, recorders, and pen registers (14);
  - —computer usage monitoring (6);
  - —electronic mail monitoring or interception (6);
  - —cellular radio interception (5);
  - —pattern recognition systems (4); and
  - —satellite interception (4).
- About 25 percent of Federal agency components responding (36 out of 142) report use of computerized record systems for law enforcement, investigative, or intelligence purposes:
  - —agencies reported a total of 85 computerized systems with, collectively, about 288 million records on 114 million persons;[4]
  - —examples of four such systems that could be used in part for data base surveillance purposes are the:
    1. National Crime Information Center (FBI),
    2. Treasury Enforcement Communications System (Treasury),
    3. Anti-Smuggling Information System (Immigration and Naturalization Service—INS), and
    4. National Automated Immigration Lookout System (INS).
  - —none of the 85 system operators provided the requested statistics on record quality (completeness and accuracy). Most do not maintain such statistics.

After conducting a review of the technology and policy history of electronic surveillance, OTA found that:

- The contents of phone conversations that are transmitted in digital form or calls made on cellular or cordless phones are not clearly protected by existing statutes.
- Data communications between computers and digital transmission of video and graphic images are not protected by existing statutes.
- There are several stages at which the contents of electronic mail messages could be intercepted: 1) at the terminal or in the electronic files of the sender, 2) while being communicated, 3) in the electronic mailbox of the receiver, 4) when printed into hardcopy, and 5) when retained in the files of the electronic mail company or provider for administrative purposes. Existing law offers little or no protection at most of these stages.
- Legislated policy on electronic physical surveillance (e.g., pagers and beepers) and electronic visual surveillance (e.g., closed circuit TV and concealed cameras) is ambiguous or nonexistent.
- Legislated policy on data base surveillance (e.g., monitoring of transactions on computerized record systems and data communication linkages) is unclear.
- There is no immediate technological answer to protection against most electronic surveillance, although there are emerging techniques to protect communication systems from misuse or eavesdropping (e.g., low-cost data encryption).[5]

OTA identified a range of policy options for congressional consideration:

- Congress could do nothing and leave policymaking up to the development of case law and administrative discretion. However, this would lead to continued uncertainty and confusion regarding the privacy accorded phone calls, electronic mail, data communication, and the like, and ignores judicial requests for clarification in areas such as electronic visual surveillance.

---

[3] The data request was sent to all major components within the 13 cabinet-level agencies and to 20 selected independent agencies. Due to the unclassified focus of this study, two Department of Defense components—the National Security Agency and Defense Intelligence Agency—along with the Central Intelligence Agency were excluded from the data request.

[4] Extent of multiple records on the same person is unknown.

[5] Technical options are being addressed in a separate OTA study on "New Communications Technology: Implications for Privacy and Security," expected to be published in winter 1986/87.

- Congress could bring new electronic technologies and services clearly within the purview of Title III of the Omnibus Crime Control and Safe Streets Act, for example by:
  - —treating all telephone calls similarly with respect to the extent of protection against unauthorized interception, whether analog or digital, cellular or cordless, radio or wire;
  - —legislating statutory protections against unauthorized interception of data communication;
  - —legislating a level of protection across all stages of the electronic mail process so that electronic mail is afforded the same degree of protection as is presently provided for conventional first class mail;
  - —subjecting electronic visual surveillance to a standard of protection similar to or even higher than that which currently exists under Title III for bugging and wiretapping.
- Congress also could set up new mechanisms for control and oversight of Federal data base surveillance, for example by:
  - —requiring congressional approval of specific Federal data base surveillance applications (e.g., by statutory amendment or approval of House and Senate authorizing committees);
  - —establishing a data protection board to administer and oversee general statutory standards for creating and using data bases for purposes of surveillance.
- Congress also could amend the Computer Fraud and Abuse Act of 1984 to cover interstate computer crime.
  - —This option, not detailed here, could provide additional legal protection against unauthorized penetration (whether for surveillance or other reasons, e.g., theft or fraud) of computer systems.[6]

Chapters 2 through 5 of this report provide technical and policy analyses relevant to proposed legislation on electronic surveillance and civil liberties, such as the "Electronic Communications Privacy Act of 1985"[7] and the "Video Surveillance Act of 1985."[8]

---

[6] See the computer crime chapter of the forthcoming OTA report on "Federal Government Information Technology: Key Trends and Policy Issues" for discussion.

[7] H.R. 3378 introduced by Rep. Robert Kastenmeier and S. 1667 introduced by Sen. Patrick Leahy. See U.S. Congress, House of Representatives, *Congressional Record*, Extension of Remarks, Sept. 19, 1985, p. E-4128; and U.S. Congress, Senate, *Congressional Record*, Sept. 19, 1985, p. S-11795.

[8] H.R. 3455 introduced by Representative Kastenmeier. See U.S. Congress, House of Representatives, *Congressional Record*, Extension of Remarks, Sept. 30, 1985, p. E-4269.

Recommended Citation:

Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington, DC: U.S. Congress, Office of Technology Assessment, OTA-CIT-293, October 1985).

Library of Congress Catalog Card Number 85-600609

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402

Senator MATHIAS. Now, I think we are in agreement that we have entered a very complex subject, and I think we are in agreement that any changes to existing law should be made only after some very careful study.

But I hope we are in agreement that the study is going to result in some action, not just study breeding more study, which is sometimes the case. Many of the issues that are in this bill are not new to this committee; we have been studying them.

Of course, we have had this bill under consideration for some time and we have consulted the Department of Justice at various points during the drafting of the bill. The subject was considered by the Attorney General in his confirmation testimony in 1984, as well as in 1985.

Now, what you have said this morning is useful and valuable, but it leaves us a little up in the air. If I were to call a markup this afternoon, I would have hoped to have a little more specific guidance from the Department.

Mr. KNAPP. Well, I think our testimony pretty much indicates, as to each specific technology or investigative tool, what it is we feel should or should not be done. And while you might not be able to mark up a bill this afternoon, you know, in a week or two you conceivably could.

I think what we are saying is, yes, some of these things should be brought under title III. Some of these technologies and tools are covered by search warrant, or should be covered by search warrant. The committee can codify that, make it clear so there is just no ambiguity about it. Fine; we have no objection to that.

Other things are not covered either by search warrant or by title III. There is no reasonable expectation of privacy; leave well enough alone, pen registers are an example. And then we make some additional procedural suggestions, some for which we have language, some for which we do not.

I think, by and large, we have given fairly good guidance as to what should or should not be considered appropriate.

Senator MATHIAS. Well, there are some areas in which you say we need more study.

Mr. KNAPP. Well, I think the one thing we have commented on is that it might be wise to await the study by the President's Commission on Organized Crime on the whole area of wiretaps before any final action is taken.

Obviously, there are a lot of new technologies; there are constantly new developments that may require some additional study. But I do think that based on the comments we have made, the committee would be in a position to write a bill. It is just that rather than being an amendment to title III, it should be maybe several bills. Amendments to rule 41, or something like that, would be preferable to trying to put everything in title III where it really does not belong.

Senator MATHIAS. I am relying very heavily on the promise of the Attorney General to help us move along in this area. You may recall that on January 30 of this year he said, "I would be pleased, if confirmed"—we closed that contract when we confirmed him—"to work with this committee to make sure that the new technology and legislation covering it conforms to the spirit of the existing laws relating to electronic surveillance." So I am cashing in that chip.

Mr. KNAPP. OK. Our people have been working with the staff of the subcommittee, I believe, and we continue to do so. We will be glad to work together to come up with a bill, or perhaps bills, which we all can support in terms of appropriate language.

Senator MATHIAS. The Attorney General talks of the spirit of the law. I am concerned that leaving electronic mail and data communications out of title III does not conform to the spirit of the law.

Mr. KNAPP. I think it clearly does because it is much more analogous to an interception of private mail right now, and that is covered by a court-ordered search warrant. There is no reason to bring it within the scope of title III, because it is not that same degree of privacy that you have with an aural communication or conversation.

When you bring something within title III, I should point out that it really creates a whole lot of additional procedural requirements and a tremendous burden. For example, we are up to about 400 to 500 wiretaps each year, which the Assistant Attorney General in the Criminal Division has to approve.

While that level is going to taper off slightly, it is still a fairly high amount. That represents two or three per working day. With that, along with everything else that the Assistant Attorney General is, by law, required to approve, plus his normal duties, you could be talking about a tremendous burden.

In addition, you have the problem that if you bring an investigative technique within title III, you would have to create a special justification for use of that technique as opposed to 7, 8, or 10 other investigative techniques which could be used.

I see no reason why that justification procedure should take place for electronic mail any more than it is required now for search warrants for business records or anything else like that.

Really, if you look at this conceptually, reading electronic mail is much more analogous to looking at financial records or, at most, looking at a citizen's private mail, which is covered by the search warrant requirements of rule 41. To change that and bring it within the scope of title III would be a tremendous change in the whole concept of what title III was designed to do, and would really seriously change the whole system, creating a tremendous burden on law enforcement without really enhancing individual rights.

We are concerned about getting courts to approve these interceptions of electronic mail just like they do now for ordinary mail. That should be more than adequate.

Senator MATHIAS. Senator Leahy, in the example that he gave you, was attempting to make it clear that the nature of the communication may be the same by electronic mail as by telephone.

Mr. KNAPP. No, because there is no aural interception involved. You do not have an ongoing, back-and-forth communication.

Senator MATHIAS. But that is what we are trying to get to, the means of communication. We are talking about the transmission of a message; we are talking about the expectation of privacy.

Why should the expectation of privacy be less in the case of electronic mail than in the case of a telephone call?

Mr. KNAPP. You have people engaged in an ongoing, direct conversation by telephone. Their voices are being recorded as they are talking about something. Electronic mail is much more like ordinary mail.

I could turn the question around. Why should electronic mail receive more protection than ordinary mail? If anything, it should receive less protection. I would have a much greater expectation of privacy if I were going to communicate anything sensitive, I would do it by ordinary mail rather than electronic mail.

Senator MATHIAS. So you are putting a blight on an industry in its infancy if you are going to tell people that they should not have an expectation of privacy in the use of electronic mail.

Mr. KNAPP. We do have an expectation of privacy, but the interception is covered by the ordinary search warrant process. That is it; that is the expectation of privacy.

STATEMENT OF FREDERICK HESS

Mr. HESS. Can I say something?

The problem, as I see it, is that you have several subjects all mixed together. If you look at the definition that is in the bill, everything is given the same protection, whether it is just the intercepting of a beep-beep, which indicates "call the office," or the placing of a listening device in someone's home or office. All these techniques are covered the same way; all the same panoply of protections are afforded.

When we start to talk in terms of electronic mail, the problem seems to be improperly getting into the system. If that is the case, on the one hand you already have protections in that we will seek a search warrant based on probable cause from a magistrate before we will permit any government agent to do it.

The other side of the coin is, what about a third party, not a governmental agent? The issue then is, should that be criminalized. If it should be criminalized, we would not have any objection to that being added either to title III or some other statute. The problem is, everything is mixed together.

Senator MATHIAS. Let me give you another example which would not involve an aural communication. Suppose I have to send a document of some kind to my Baltimore office and it has to get there in a matter of minutes. I put it on a facsimile machine and it is transmitted to the Baltimore office.

Now, that is not an aural communication, but that may be a highly confidential, very personal document. Do I have an expectation of privacy, although it is not an aural communication?

Mr. KNAPP. Absolutely, and therefore it is covered by rule 41.

Mr. HESS. When I am asked that question in terms of interception, that is the answer I give. You need a search warrant. It is not covered by title III, but you need a search warrant.

Senator MATHIAS. All right, but is it not true that interception of that transmission might not be a violation of title III, as it now exists?

Mr. KNAPP. Right.

Mr. HESS. That is correct.

Senator **Mathias**. All right, so I do not have that expectation of privacy.

Mr. **Knapp**. Yes, you do. Title III is not designed to be the sole mechanism for ensuring an individual's expectation of privacy. It is only one particular vehicle, one of several vehicles which is provided by Federal law. The most traditional and the most meaningful one is obviously the fourth amendment itself and the requirement for a search warrant.

Senator **Mathias**. I want to be sure I understand exactly what your testimony is and what the Department's position is, because I think it is very important. You object, as I understand it, to requiring a warrant under the wiretap law, title III, to intercept electronic mail?

Mr. **Knapp**. Right, under title III, but we have no objection—in fact, it is the law that it is required now under——

Senator **Mathias**. But you agree that an ordinary search warrant ought to be required?

Mr. **Hess**. It is.

Mr. **Knapp**. We feel it is required and we have no objection to the committee drafting legislation which restates that requirement to resolve any ambiguity that exists.

Senator **Mathias**. All right. Now, very specifically, why do you object to title III coverage for electronic mail? You talk about enormous burdens. What additional burdens would be imposed on law enforcement beyond that required to obtain a search warrant?

Mr. **Knapp**. There are several things which title III does which rule 41 does not do. First, and it has been highlighted, is the title III requirement that you have a headquarters review and approval before the technique is even utilized. That requirement goes all the way to a personal approval by the Assistant Attorney General of the Criminal Division. That is a very time-consuming process. That is No. 1.

No. 2, there is a minimization requirement. When you are talking about a search warrant to intercept mail or a specific document that is being transmitted by facsimile or whatever, that is sort of self-minimizing. Whereas an aural communication is something which goes on and on and which could conceivably get into topics that are unrelated.

You need a minimization requirement in that, so that is why you have special title III provisions on minimization.

Third, because the interception of aural communications and confidential communications on the telephone was deemed by the Congress in 1968 to be such a very sensitive thing, there is a requirement that we show that other alternative investigation techniques are not feasible.

Well, I do not think that requirement to get a search warrant should be imposed on electronic mail, particularly where you are talking about data communications.

Fourth, title III is restricted only to cover certain kinds of offenses, and only the most major ones dealing with organized crime and drug trafficking. There is no need for such a restriction for electronic mail communications.

Again, we believe that the requirements of rule 41—the requirement that there be probable cause to believe an offense has been committed and that the document, or whatever is being intercepted, is relevant to proof that a particular crime has occurred; approval by a judge; a written order; an affidavit and everything—all those protections are fully adequate to ensure the privacy of the people who are involved in the communication. This is the same protection which is afforded now for ordinary mail.

Senator **Mathias**. What we are reaching for in this bill is to protect the transmission without respect to the technology. Now, I gave you the example of putting a document on a facsimile machine and sending it to my Baltimore office.

Mr. **Knapp**. Yes, sir.

Senator **Mathias**. As an alternative, I could have picked up the phone and dictated it to a stenographer in my Baltimore office. Now, the transmission would have been identical; the communication would have been identical. The only thing that would be different would be the technology I employed. Why should one have title III protection and the other not?

Mr. **Knapp**. Again, because——

Mr. **Hess**. Historically, the telephone has had that protection; it has had it since 1968.

Senator **Mathias**. Well, we are trying to overcome history now and to face life as it really is.

Mr. **Knapp**. You could have also made that communication by letter, or you could have met the person in a public place and discussed it with him and someone could have overheard you. In each situation, there is a historical reason for it.

We believe that the search warrant is more than adequate protection for your privacy.

Senator **Mathias**. I could have met the person face to face; I could have arranged to have a rendezvous in a plowed field, which is the safest place in the world to exchange confidences. [Laughter.]

But the law attempts to move us out of that barbaric climate and to make it possible for civilized people to communicate with the expectation of privacy. Now, I find it very difficult to agree that you are going to confine that to a specific technology.

Mr. **Hess**. Senator, when you send that document, you send that document, and that document only. When you get on that telephone and dictate it, something else can happen. Further conversation can occur. The secretary on the other end can ask if her friend is in the office and then talk to her for a minute.

All kinds of things can happen during that telephone conversation that cannot happen when you just send a piece of paper by an electronic means instead of putting it in an envelope.

It is the same paper, it is the same information, but it becomes very different when it is over the telephone because it is literally open-ended. That, I think, is the reason title III is different for telephone calls and that is why Congress never put ordinary letters into title III.

Senator **Mathias**. Well, you have somewhat changed my hypothesis.

Mr. **Knapp**. I think it is self-minimizing, typically. Your typical electronic mail or any type of mail communication is self-minimizing and you are not talking about an ongoing thing that is going to continue for a period of time like with a typical wiretap, which involves an aural communication.

Senator MATHIAS. Since Senator Leahy raised this same issue in his questions, let me yield to him for a question.

Senator LEAHY. Thank you, Mr. Chairman. I also want to thank Mr. Knapp for agreeing to work with the subcommittee staff and hopefully develop a bill that we can all support. We all know, with how the Senate schedule works that if we have a consensus bill, how much easier it is going to be to get it through.

In your testimony you say that title III has proven itself amenable to application to a number of new technologies, although not all those that have been developed. Let me make sure I understand. Is title III applicable to data transmissions?

Mr. KNAPP. Not to data transmissions where there is no audio involved.

Senator LEAHY. Is it applicable to the transmission of video images?

Mr. KNAPP. No. Again, there is no audio involved. However, the search warrant, rule 41, is applicable.

Senator LEAHY. But does rule 41 apply if title III is not applicable to the transmission of video images?

Mr. KNAPP. Pardon?

Senator LEAHY. If title III is not applicable to the transmission of video images, why would you need a search warrant?

Mr. KNAPP. You would need it because there is a reasonable expectation of privacy involved, and therefore you need a court order. That is a requirement that comes from the fourth amendment. Title III imposes additional requirements over and above what the fourth amendment and rule 41 require for certain types of communications. Congress felt it was appropriate to add some additional safeguards.

Senator LEAHY. If we did not have title III, would you be able to just have wiretapping?

Mr. KNAPP. You would have to get a court order.

Mr. HESS. Senator, the phrase you read dealt with telephone conversations. There are very few telephone conversations that go on, voice conversations, that we feel are not now covered by title III.

The only telephone conversations that I can think of that are not in whole or in part by wire might be those from a car phone to a car phone.

Senator LEAHY. I understand. If you did away with title III, would you be able to just tap those wires?

Mr. HESS. We would still need a court authorization. If there were no title III at all and we wanted to do it, we would probably have to test the whole concept in court again, but we would start with a court order in the nature of a search warrant based on probable cause.

From our experience, if title III vanished tomorrow, we would insist that all the protections in title III get put into that court order. That is what is happening now with closed-circuit television.

Senator LEAHY. Do you think title III is applicable to a voice conversation carried on over a private telecommunication network? A lot of big corporations might go from building to building or even from city to city.

Mr. **Knapp**. If there is any wire involved, yes.

Mr. **Hess**. Not necessarily, because it is not affecting commerce.

Senator **Leahy**. Suppose you have got city A and city B both within the same State. What you do is you send this by microwave. You have got one building in this city, one building in the next city—I mean, this is going on all the time now—and the corporation decides, especially after the great improvements after the breakup of AT&T, that now what they do is they send their own microwaves back and forth.

Is title III applicable to that voice conversation?

Mr. **Hess**. I do not believe that it currently is, and that is precisely the type of area we would like to work with the committee on. We would rather do it individual problem by individual problem because they are not all the same.

The degree of invasion of privacy is different in each case and you have to determine whether or not it rises to the level where it ought to be in title III, with all its complicated panoplea of protections.

Senator **Leahy**. Now, if title III was repealed tomorrow, you would still go for court orders, is that correct?

Mr. **Knapp**. Yes; we have to.

Mr. **Hess**. It is an investigative technique that is absolutely essential.

Senator **Leahy**. Now, let me ask about the private citizen. Do you think title III is any kind of a deterrent to interception of telephone conversations by private parties?

Mr. **Hess**. It certainly is; it is a crime. It is illegal to wiretap unless you have a court order.

Senator **Leahy**. If you did away with title III tomorrow, would there be any significant deterrent to interception of telephone conversations by a private person?

Mr. **Hess**. Well, I do not advocate getting rid of title III tomorrow or any time in the near future.

Senator **Leahy**. I think you are missing the direction of my question. I am trying to talk about what we need here for legislation.

If you did away with title III—and I know you are not advocating it; I am not advocating it. Nobody is advocating doing away with it, but I am trying to make sure I understand this. You are the expert; I am just a lawyer from a small town in Vermont.

If you did away with title III tomorrow, would there be any deterrent to the interception of telephone conversations by private parties?

Mr. **Hess**. Not that I am aware of.

Senator **Leahy**. So even though you feel the fourth amendment or something like FISA or the Federal Rules of Criminal Procedure might apply to Federal authorities in tapping into the various examples I have given you, the prohibitions on private interception of the new forms of electronic communication are petty nonexistent, are they not?

Mr. **Hess**. Yes, and I think there has to be a distinction made between regulation of what the Government does and regulation of what private citizens can or cannot do. The problem of the gaps that exist in law, to me, primarily is the current lack of a method of regulating what private citizens can do to intercept communications with the new technologies. The Government at least is seeking a court order based on probable cause to intercept almost anything we have discussed here.

Senator Leahy I do not have any problem with that, but what I am saying is if we have a responsibility in this committee, it is to protect the anticipated privacy that you have.

I mean, if I am the head of that hypothetical company that I gave you and I am sending data transmissions or anything else to somebody else, I anticipate privacy in doing that. I anticipate it from the Government, but I also anticipate it from my competitors or just a snoop.

What I am trying to do is to make sure that our legislation keeps up with these enormous changes in our telecommunications that have taken place in the last few years. When you talk to the best experts and say tell us exactly what we will have 10 years from now, they cannot because the state of the art changes with a geometrical progression.

What I want to do is make sure this legislation protects the legitimate fourth amendment interests that we anticipated under title III. But that is just one part.

I also want to make sure we put enough teeth in there so that unscrupulous competitors cannot just steal things willy-nilly. Of course, a lot of data now—blueprints and everything else—get sent this way. We also want to provide that a snoop, malicious or otherwise, cannot lawfully intercept these data communications. In other words, to give people just about the same level of privacy protection that we used to have when we picked up Ma Bell.

Mr. **Knapp**. We would have no objection to such legislation, but it should be separate legislation, not part of title III, because title III governs conduct both by the Government and individuals.

We believe that, as to the type of technologies we are talking about here, the search warrant process should be adequate for Government conduct. Therefore, anything to restrict eavesdropping by private citizens should be handled by separate legislation.

Senator **Leahy**. But that is what I do not understand. If you eavesdrop on my state-of-the-art phone system that transmits in digital form, why should you be any different because title III did not cover that or anticipate it?

Why should it not anticipate it? It is the same thing; I am doing the same kind of communication.

Mr. **Knapp**. I think title III does cover that if there is any wire involved, and we would have no objection to expanding title III to cover a strictly digitized radio communications, as I explained in my testimony, between two telephones. We would have no objection to expanding title III to that extent.

I think the written statement pretty much lays out that if it is a digitized communication between telephones, even if no wire is involved, we would have no objection to expanding title III to cover that.

Senator **Leahy**. Well, we are coming closer together on this, but I do not want to be in a situation that people feel that the only way they have protection both against individuals and Government is that they have got to go down to the Smithsonian and get an old phone system out to have it.

Senator **Mathias**. While we are on title III, I think it is important to have a clear understanding of what we are thinking about. I perceive title III as somewhat of a two-edged sword.

It authorizes interceptions of phone communications under certain circumstances, but it also, with the other edge of the sword, outlaws any interceptions that are not made pursuant to those particular circumstances.

Now, in your statement you have focused on the first edge of the sword, the authorized interceptions and the circumstances under which the law enforcement officials may intercept.

Mr. **Knapp**. Yes, sir.

Senator **Mathias**. But there is the other edge that we have to consider, and that is the prohibition against unauthorized interceptions.

Mr. **Knapp**. Yes.

Senator **Mathias**. What about electronic mail? Is it the position of the Department that it should be a violation of law to intercept messages that are transmitted by electronic mail?

Mr. **Knapp**. By private citizens, yes.

Senator **Mathias**. But not by the Government?

Mr. **Knapp**. The Government is covered by the search warrant process, and we believe that that should be the methodology for getting court-authorized approval.

Senator **Mathias**. Well, is it presently a violation of law to intercept electronic mail?

Mr. **Knapp**. It would be a violation of the fourth amendment for the Government to do that.

Senator **Mathias**. Flat out?

Mr. **Hess**. That is the policy we follow. We are simply not going to intercept without a court order.

Senator **Mathias**. I am not talking about a policy. I am talking about the law. Is it against the law.?

Mr. **Knapp**. It is against the fourth amendment, and we are bound by the Constitution. Yet, there is no specific statute which specifically prohibits it. Therefore there is clearly a gap for activity by individuals, but there is no gap for activity by Government agents. It is clearly under the coverage of the fourth amendment, which means that a search warrant is required.

Senator **Mathias**. But it would also be a violation of statute if it were an aural communication?

Mr. **Knapp**. That is correct.

Senator **Mathias**. Now, that, I think, is the question that Senator Leahy and I still have. Why should we continue a distinction between aural and nonaural?

Mr. **Knapp**. Well, again, your typical wiretap involves an order to cover conversations that could be going on for a period of time where you have new elements coming in, irrelevant topics. The interception is going to go on for 30 days or something like that.

In a search warrant for electronic mail, you are talking about a search warrant for a specific communication. It is self-minimizing. It is a more commonly used investigative technique because search warrants for specific items of evidence, be it electronic mail, bank records or anything else, are self-minimizing.

It is narrow in focus and it is not the sort of thing, because it is not ongoing, that should be a sort of last-resort type of investigative technique.

On the other hand, you are talking about aural communications where, as Mr. Hess pointed out, you could have irrelevant topics brought into the conversation. It could get well beyond the scope of the initial communication.

Typically, it is not just for one communication; it is for a series of communications over a telephone for a 30-day period. You are talking about an ongoing invasion of privacy which is not self-minimizing, and you therefore need the additional protections and procedures provided by title III.

To impose title III's four or five additional protections, which I summarized earlier, on all types of electronic mail would just totally radicalize current law and seriously impede law enforcement because you would now be talking about—I do not know—several thousand such requests every year.

Senator MATHIAS. Well, now, almost every office today has a device on the telephone for recording messages.

Mr. KNAPP. Yes.

Senator MATHIAS. What is the legal position of those recorded messages?

Mr. HESS. If somebody is on a telephone, leaving a message on a recorder, and somebody is intercepting, as far as I am concerned, that is covered by title III. There is an aural message that can be heard with the ear being given to the machine, from a human being to a machine.

If it is being intercepted by the Government, we ought to have a title III search warrant. If it is being intercepted by an individual person, he is committing a crime.

Senator MATHIAS. So if I record my words on a tape, you think it is covered, but if I record my thoughts on a piece of paper, it is not covered?

Mr. HESS. If you seal that piece of paper and put it in the mail, I will need a search warrant to open it. If you leave it in your office and I want to read it, I need a search warrant, as a Government official, to come in and search for it and get it. So to that extent, it is covered.

If you leave it in such a position that an ordinary citizen finds it——

Senator MATHIAS. I put it on a facsimile machine and send it.

Mr. HESS [continuing]. And if the Government wants to read it, we feel there is an expectation of privacy involved in it and you have to have a court order issued by a magistrate based on probable cause before the Government can see it.

The only things that are missing are some of the extra protections of title III. Amongst them is the review procedure that goes on in Washington that I supervise, which is extremely complex.

It is complex because a telephone conversation is historically different. It can expand; it can go into other things. It is not just the individual piece of paper that is on a facsimile machine.

Senator MATHIAS. But the Department's position is that nonaural communication is basically outside of title III and ought to be outside of title III?

Mr. HESS. Yes, the way the law is written.

Senator MATHIAS. Can you think of any other new technologies to which title III ought to apply? You have already mentioned digital telephones that may not have a wire link.

Mr KNAPP. Yes. If you try and visualize something that is analogous to a telephone that, for some reason, does not involve wire—perhaps there is some sort of radio wave communication or something like that which is encrypted in such a way that it shows that the person intended it to be a private communication—I would say yes.

There are some new technologies that do not strictly involve wire which perhaps should be covered by title III, and I think that is made clear in my testimony, if it is a communication digitized in some form.

Senator MATHIAS. That is your example of a new technology that ought to be included?

Mr. KNAPP. Yes. Car telephone to car telephone.

Senator MATHIAS. Right.

Mr. KNAPP. Anything that is like a telephone; if you júst think of it conceptually, it is very much like a telephone.

Mr. HESS. If the person on the phone line conceives that he is talking on the phone, it does not matter if it is from a car phone or whether it is being bounced off a satellite or microwave or whatever.

Ordinary citizens on a telephone consider a telephone to be a telephone, and that is the thing that title III protects. If title III has gaps in it, that is the kind of thing that ought to be amended by Congress.

Senator MATHIAS. But if I query my office in Baltimore with a memo and they answer with a memo, that is different?

Mr. KNAPP. It is a specific, self-limiting communication. It is just like ordinary mail.

Mr. HESS. And we are not objecting to criminalizing individuals getting into it. The Government is restricted now in getting into it.

Senator MATHIAS. Well, we could carry this on all morning with great interest. We have a number of other witnesses that we need to hear. But to see if we can summarize it, what you are suggesting in your testimony is that the analogy for electronic mail is conventional first-class mail.

Mr. KNAPP. Yes.

Senator MATHIAS. You point out that the Government needs a search warrant under rule 41 of the Federal Rules of Criminal Procedure to intercept and open a letter which is mailed through the postal service.

Mr. KNAPP. Yes.

Senator MATHIAS. Now, in that warrant you can say, I think that Charles Mathias wrote a letter on November 13, 1985, sitting in his office in the Russell Office Building, and that he personally carried it downstairs and put it in a letter box on the corner of Constitution and First Streets, and we want to see that letter.

Mr. KNAPP. You are going to need a lot more than that before you get a search warrant. You cannot think anything. First of all, you are going to have to show that it is relevant to a crime and that you have probable cause to believe that it is relevant to a crime.

Senator MATHIAS. All right. You are singing my song now. How are you going to particularize a piece of electronic mail in that way?

Mr. KNAPP. The same way you would for ordinary mail. Whatever information you have—I do not know; it could come from an informant who saw you write the letter; I saw Charles Mathias outline a scheme to steal money from a bank, or something like that, and it is all contained in the letter and it is going to show how he plans to commit a robbery in 5 days, or something like that.

Senator MATHIAS. But how do you extract that from electronic mail, which is an ongoing process. The message is not a static object, like a piece of paper confined in an envelope that can be identified. These are bits and bytes.

Mr. HESS. That depends on the technology and the ability of the people who are doing it to intercept and to know when a certain document is going. The better example is if two narcotics dealers are communicating with their own computers and sending information back and forth as to who owes them what money for how many kilos of whatever.

If we had enough information to believe that there was probable cause to believe they were doing that in the context of that offense and that they were doing it on a computer line without an aural communication, we would seek a court order from a magistrate based on probable cause to believe they were engaging in this type of conversation and seek to intercept those messages.

It is very difficult to pick one message out of a hat. You have to know where it is going to, from whom, what time.

Senator MATHIAS. Well, this is all so interesting, I find it very difficult to bring it to a halt. You mention in your statement that tracking devices are being increasingly used by courts. They are an alternative to incarceration.

You have reservations about applying this bill to tracking devices. Do you think that the provisions of the bill would inhibit experimenting with this form of punishment for crime?

Mr. KNAPP. Tracking devices—as the law is now, there is no constitutional problem unless you are going to go into an area of privacy like a home or something like this, in which case a warrant would be required.

A tracking device is more analogous to following someone. A police officer might trail a drug trafficker, and follow him in a car or something like this. Instead of doing that, a tracking device is put on the car or on the individual.

In that situation, since it is more analogous to an investigator just following him, there is no requirement for a warrant.

Mr. HESS. Senator, are you referring to a sentence of imprisonment to your home with a tracking device on your leg?

Senator MATHIAS. Yes, a sentence to wear a tracking bracelet of some kind.

Mr. HESS. Well, I do not think there is any problem there because you are dealing, in essence, with the consent of the person. At some point he has got to, I would assume, consent, or at least it is subject to a court order requiring this as part of the sentence, one way or the other. So I do not think there is a problem there.

Senator **Mathias**. Well, my question is do you think that the provisions of this bill would inhibit experimental——

Mr. **Knapp**. If you have to get a court order for every tracking device which DEA or the FBI wanted to use, it would seriously impede law enforcement. They would spend all their time preparing affidavits and the upshot would be that they would not use tracking devices. They would end up just trying to follow people themselves, which could be very dangerous and certainly not always very effective.

Senator **Mathias**. And you also, on page 14, mention pen registers. Is it your position and the position of the Department that there is no statutory requirement for court supervision of a pen register?

Mr. **Knapp**. FISA requires it.

Mr. **Hess**. The FISA statute, in all probability, the way we read it, requires a court order for a pen register.

Senator **Mathias**. In all probability?

Mr. **Hess**. Yes, but it does not require a court order based on probable cause. You do not get the contents of a conversation from a pen register. One of my problems with the definition in the bill is that almost everything is lumped together.

A pen register just indicates that a number was dialed from a phone to another phone, the time of day and how long it went on. It does not indicate who called, who was on either end of the phone, or any contents of the conversation.

Senator **Mathias**. Senator Leahy has been called away to another committee. He and I both have some further questions and I think in the interests of time, we should submit those further questions to you.

Mr. **Knapp**. We will be glad to do so.

Senator **Mathias**. Let me ask you this further oral question. I was serious when I said the Senate is considering buying a new telephone system. I want to know what is the legal position of digital phones if we install them here in the Senate today.

Mr. **Knapp**. Again, if there is any sort of wire communication involved, it is clearly covered by title III. If there is no wire, but there is a strictly digitized radio communication, it would require a search warrant. But you are right; there is a gap there and that ought to be brought into title III.

Senator **Mathias**. We appreciate your statement of policy on that subject.

Mr. **Knapp**. Well, it is more than a statement of policy.

Mr. **Hess**. It is more than that.

Mr. **Knapp**. It is the statement of the law; we believe that is the law.

Mr. **Hess**. If this conversation on these Senate phone systems—and I am no expert in this digitized business—is in whole or in part by wire, as that term was understood in the 1968 statute, then it is covered by title III.

If it is some sort of a system that is not all or in part by wire or cable, as that definition exists today, then theoretically, probably, it is not covered. But the Senator is on the phone; he is talking with a human voice and he is hearing a voice on the other end. He has a phone with a wire connected to something.

That wire probably comes from, whether it is digitized or not, a phone company, which is a commercial common carrier, unless the Senate is planning to buy its own independent phone system that it owns and no other common carrier is involved, which I assume is not the case.

Senator MATHIAS. Do not assume anything in this technological revolution. [Laughter.]

Mr. HESS. Assuming that, it is covered.

Senator MATHIAS. Well, we are a little sensitive, you know. I remember the late, great Emmanuel Celler used to be the chairman of the House Judiciary Committee. He used to look around the committee room, and he would say, "They have dossiers on every one of us and they will use them if it suits their purpose." It turned out he was right, because I went down and looked at mine. We do not want to encourage the accumulation of another system of dossiers.

I think it would be very useful for us to have an informal session with the Justice Department and the committee to look at some of the further drafting problems we have here. I am calling in my marker with the Attorney General on that subject. I think we need to make progress because the scientists and engineers and electronics experts are ahead of us, and if we have any hope of catching up, we have got to start.

Thank you very much for being here.

Mr. KNAPP. You are welcome. Thank you.

[The following survey was subsequently received for the record:]

PROSECUTIVE RESULTS OBTAINED IN INVESTIGATIONS UTILIZING ELECTRONIC SURVEILLANCE (WIRETAPS)

Prepared by:
Office of Enforcement Operations
Criminal Division
Department of Justice
April 25, 1986

SUMMARY

The Office of Enforcement Operations recently completed an evaluation of the prosecutive results obtained in cases utilizing electronic surveillance or "wiretaps." The evaluation encompassed approximately 35 percent of electronic surveillance requests approved during 1983. For evaluative purposes, the electronic surveillance requests were grouped together in discrete investigations.

The Office of Enforcement Operations found that of the 51 investigations in its survey, 38 had resulted in at least one conviction, seven were pending at either the trial or investigative stage, and six were unsuccessful, not resulting in any convictions. The six unsuccessful investigations, however, were small in relation to all other cases with an average of 2.8 interceptees compared to an average of 12.1 interceptees for all other cases. Indictments had been returned in four of the seven pending cases and indictments were expected in the other three pending cases. If indictments are returned in these three cases

as expected, 88 percent of the 51 investigations will have resulted in at least one indictment.[1]

A total of 181 interceptees and 287 non-interceptees were either convicted or plead guilty in the 44 completed investigations. This averages to 10.6 convictions for each completed investigation. The median period of incarceration (exclusive of the approximately 15 percent who received only a fine and/or probation) for interceptees and non-interceptees was 5.4 years and 3.3 years respectively. Finally, 78 of the guilty defendants had fines levied against them totalling more than $900,000.

Another significant statistic revealed by the survey was the great success enjoyed in those cases in which a targeted interceptee was indicted. Excluding pending prosecutions and fugitives, over 95 percent (181 of 189) of the final dispositions resulted in a conviction or a plea of guilty by an interceptee who was indicted. The other eight were accounted for by seven dismissals and just one acquittal. The 95 percent guilty rate compares favorably with the 83.7 percent guilty rate for all 1983 federal felony prosecutions. This 11.3 percent difference is not entirely explainable by the existence of a wiretap because other investigative tools, like informants and longterm undercover operations, are frequently involved as well in these major investigations, but it is clear that the almost irrefutable evidence developed through a wiretap is largely responsible for this high guilty rate.

Finally, consistent with overall law enforcement initiatives, 75 percent (38 out of 51) of the investigations surveyed were drug related. A complete breakdown of the types of investigations in which electronic surveillance was used is as follows:

---

[1] For comparative purposes, a February 1984 study released by the Bureau of Justice Statistics showed that only about 50% of the matters received by United States Attorneys are eventually filed as felony cases. The relationship between matters and felony filings is analagous to the relationship between investigations and indictments.

Type of Case	Number of Cases[2]
Drugs: Cocaine	23
Drugs: General	9
Drugs: Marijuana	8
Drugs: Methamphetamine	8
Drugs: Heroin	7
Gambling	5
Loansharking	5
Theft	5
Public Corruption	4
Murder Conspiracy	2
Explosives	2
Counterfeiting	1
Insurance Fraud	1

More detailed dispositional and sentencing information and a more complete description of the evaluation's methodology are contained in the appendices to this report.

APPENDIX 1

EVALUATION METHODOLOGY

The Office of Enforcement Operations initially drew a computer-generated random sample of 63 of the 208 original electronic surveillance requests approved during calendar year 1983. Seven of the original sample wiretaps were eliminated because they were actually initiated before 1983. Five more of the original sample were found to be related to other wiretaps within the sample and were grouped together. An additional 17 wiretaps originally outside the sample were included in the sample because they were found to be related to sample wiretaps.

The Office of Enforcement Operations decided to evaluate related electronic surveillances together because this process provided a way to eliminate double counting of the same person on separate wiretaps and because the grouping corresponded more directly to discrete prosecutions than would evaluating each wiretap separately. At the conclusion of this process, the Office of Enforcement Operations had a sample of 51 separate investigations encompassing 73, or 35 percent, of the 1983 wiretap authorizations.

---

[2] The total number of cases is greater than 51 and the total that are drug-related is greater than 38 because many cases fell into more than one category.

For each investigation identified, the Office of Enforcement Operations decided to track the prosecutive results of all interceptees named in the sample and related or spinoff requests. This turned up a total of 549 separate interceptees. Letters were sent to the United States Attorney in each federal district where there was an investigation within the evaluation sample. When no response or an incomplete response was received, a telephone call to the applicant attorney was made. This resulted in a 100% response rate although some dispositions for particular interceptees/defendants were missing, largely as a result of pending investigations. Prosecutive information was also requested for persons who were not named as interceptees but were nevertheless indicted as a result of the investigations in the sample.

The Office of Enforcement Operations initiated its own evaluation of prosecutions using electronic surveillance because it believes the existing reporting mechanism, by design, fails to fully capture the benefits obtained through the use of electronic surveillance. A description of the existing reporting mechanism follows.

The Omnibus Crime Control and Safe Streets Act of 1968, the electronic surveillance statute, requires the applicant attorney to submit information regarding prosecutive results of approved electronic surveillance requests. The attorneys' reports are submitted to the Administrative Office of the United States Courts which, in April of each year, transmits to Congress a comprehensive report of the previous year's activity.

The Administrative Office of the United States Courts has to rely on complete and accurate reports from the attorneys to compile its prosecution statistics. Because of the April reporting date, most of the prosecutions which used electronic surveillance from the previous year are incomplete. As a result, attorneys are expected to send in subsequent prosecutive reports, sometimes, two, three, or four years after an electronic surveillance has terminated. A significant amount of information is never reported because of the lapse in time between the actual electronic surveillance and the prosecution. Experience indicates that follow-up reporting by the prosecutors is not done uniformly through no fault of the Administrative Office of the United States Courts. Compounding this problem is confusion over whether subsequent reports should be prepared "net" of previously reported results or cumulative with previously reported results. Finally, the statutory reporting requirements do not specify that convictions be tied to original interceptees or that sentences of convicted defendants be enumerated. These reasons led the Office of Enforcement Operations to initiate its own evaluation.

APPENDIX 2

DETAILED DISPOSITIONS OF INTERCEPTEES

A total of 549 interceptees were identified in the 51 investigations within the survey sample. The dispositions for the 549 interceptees are detailed below.

	Number	Percentage
Convicted/plead	181	33.0
Dismissed	7	1.3
Acquitted	1	.2
Indicted, but pending or fugitive	59	10.7
Not indicted, but investigation continuing	42	7.6
Never indicted	232	42.3
Deceased	3	.5
No information/other	24	4.4
Total	549	100.0

A large number of interceptees are never indicted. Statutory construction and a conservative interpretation of case law require applicant attorneys to list as an interceptee any person if there is probable cause to believe that the person is committing, has committed or is about to commit an enumerated offense in the statute and if there is probable cause to believe that the person will be intercepted. This inclusiveness is intended to better protect the rights of those who may be intercepted because of the statutory requirement that named interceptees be notified that their conversations were surveilled. One Circuit Court of Appeals case has specifically enjoined the Government to err on the side of naming more interceptees for these reasons. [See United States v. Martin, 599 F.2d 880 (9th Cir. 1979)]. The Office of Enforcement Operations specifically follows the dictates of this decision. In addition, as a practical matter, the decision to indict implies that evidence of a much higher order (sufficient to gain a conviction) be available than the evidence required to obtain a court order to employ electronic surveillance at the investigative stage (probable cause). Finally, some of the interceptees may have been used later as witnesses in cases where their relative culpability was slight and their testimony deemed more useful to convict more culpable parties. Combining these reasons explains the 42 percent rate of non-indictment for the total class of interceptees. Similar attrition rates were found in a September 1985 study released by The Bureau of Justice Statistics which found that a median of 49 percent of the felony arrests (probable cause) in ten jurisdictions were dismissed or rejected for prosecution. Finally, as mentioned earlier, 95 percent of the interceptees who were indicted were eventually convicted or plead guilty.

APPENDIX 3

SENTENCING INFORMATION - INTERCEPTEES

Sentencing information for 16 of the guilty interceptees was unknown or pending. The remaining 165 guilty interceptees' sentencing information is detailed below:

Sentence Imposed	Number	Percent
Fine only	1	.6
Probation only	21	12.7
Less than 1 year	17	10.3
1 - Less than 2 years	16	9.7
2 - Less than 4 years	13	7.9
4 - Less than 6 years	36	21.9
6 - Less than 8 years	14	8.5
8 - Less than 10 years	6	3.6
10 - 15 years	23	13.9
Less than 15 - 20 years	10	6.1
Less than 20 years	7	4.2
Life	1	.6
Total	165	100.0

Excluding those who received only a fine and/or probation, the median sentence of incarceration imposed on this group of interceptees was 5.4 years.

In addition to the sentences detailed above, 23 interceptees received a special parole term and 28 interceptees received a term of probation in addition to their imprisonment. A total of over $400,000 in fines was also levied against 32 interceptees.

To give this sentencing information a benchmark for comparison, it is necessary to compare similar sentencing information for other groups of guilty defendants. The United States General Accounting Office (GAO) performed a similar analysis for 1983 federal felony, 1981 strike force, and witness security prosecutions.[3] A breakdown of the sentencing outcomes for the three GAO prosecution groups and the interceptee group is listed below.

---

[3] Witness Security Program: Prosecutive Results and Participant Arrest Data (August 23, 1984, GAO/GGD 84-87), pp. 16-17.

	1983 federal felony	Strike force	Witness Security	Interceptees
	(percent)			
Sentence imposed				
Probation only	38	26	16	13
Less than 2 years	26	30	14	20
2 years or greater	36	44	70	67
Total	100	100	100	100

While GAO in its report correctly urges that caution should be used in comparing sentences handed out between the different prosecution groups, it is nevertheless apparent that the interceptee prosecution group received significantly more severe sentences than the 1983 federal felony and strike force groups and essentially equivalent sentences as the witness security group.

APPENDIX 4

SENTENCING INFORMATION - NON-INTERCEPTEES

The Office of Enforcement Operations also asked applicant attorneys to detail prosecutive results for people who were not named as interceptees but were nevertheless indicted in the 51 survey investigations. This part of the survey turned up an additional 287 "non-interceptees" who were convicted or plead guilty. Excluding 20 guilty non-interceptees for whom sentencing information was unknown, a breakdown of the sentencing information for the remaining 267 non-interceptees is as follows:

Sentence Imposed	Number	Percent
Fine only	1	.4
Probation only	49	18.4
Less than 1 year	44	16.5
1 - Less than 2 years	30	11.2
2 - Less than 4 years	55	20.6
4 - Less than 6 years	41	15.4
6 - Less than 8 years	9	3.4
8 - Less than 10 years	14	5.2
10 - 15 years	19	7.1
Less than 15 - 20 years	3	1.1
Less than 20 years	2	.7
Life	-	-
Total	267	100

Again, excluding those who only received a fine and/or probation, the median sentence of incarceration handed out to the non-interceptees was 3.3 years. In addition to the above sentences, 28 non-interceptees received a term of special parole and 42 non-interceptees received a term of probation in addition to incarceration. Finally, a total of over $480,000 in fines was levied against 46 non-interceptees.

APPENDIX 5

STATISTICAL SUMMARY OF CONVICTIONS IN THE 51 SURVEY INVESTIGATIONS

	-------CONVICTIONS-------		
CASE NUMBER	INTERCEPT	NON-INTER	TOTAL
1	0	0	0
2	2	0	2
3	3	17	20
4	6	2	8
5	4	1	5
6	4	0	4
7	3	11	14
8	2	11	13
9	3	1	4
10	3	0	3
11	5	0	5
12	6	0	6
13	3	3	6
14	6	15	21
15	4	5	9
16	4	0	4
17	1	1	2
18	0	0	0

CASE NUMBER	CONVICTIONS		
	INTERCEPT	NON-INTER	TOTAL
19	16	24	40
20	0	19	19
21	0	0	0
22	6	11	17
23	8	4	12
24	9	48	57
25	0	0	0
26	4	5	9
27	0	0	0
28	0	14	14
29	0	0	0
30	2	2	4
31	0	0	0
32	14	31	45
33	3	5	8
34	0	0	0
35	0	0	0
36	2	3	5
37	0	0	0
38	12	0	12
39	6	0	6
40	0	0	0
41	6	21	27
42	0	0	0
43	6	3	9
44	4	2	6
45	2	3	5
46	2	12	14
47	0	8	8
48	3	0	3
49	0	0	0
50	9	4	13
51	8	1	9
TOTAL	181	287	468

Senator MATHIAS. Our next witnesses, we will ask to appear as a panel: Mr. Philip Walker, the vice chairman of the Electronic Mail Association; Mr. Michael Nugent, chairman of the Privacy Committee of the Association of Data Processing Service Organizations; and Mr. John Stanton, chairman of the Telocator Network of America.

Gentlemen, as you can see, as a result of interruptions and other matters, we are a little behind schedule. If you could keep your oral statements as brief as possible, 5 minutes or less, your full written statements will be printed in the record.

Who would like to start?

STATEMENT OF A PANEL, CONSISTING OF PHILIP M. WALKER, VICE CHAIRMAN, ELECTRONIC MAIL ASSOCIATION, WASHINGTON, DC; P. MICHAEL NUGENT, CHAIRMAN, COMMITTEE ON COMPUTER SYSTEMS AND COMMUNICATIONS PRIVACY, ASSOCIATION OF DATA PROCESSING SERVICE ORGANIZATIONS, ARLINGTON, VA; AND JOHN STANTON, CHAIRMAN, TELOCATOR NETWORK OF AMERICA, WASHINGTON, DC

Mr. WALKER. Good morning, Mr. Chairman. I am Philip M. Walker, general regulatory counsel for GTE Telenet, Inc., one of the Nation's leading providers of packet switch telecommunications and electronic mail services.

I am appearing today as vice chairman of the Electronic Mail Association. The association is a Washington-based trade group created 2 years ago by many of the leading companies in the electronic mail field.

We now have over 60 members spread throughout the United States and Canada, and several European companies as well. Electronic mail is a product, an application of the melding of computer and communications technology. It allows virtually instantaneous communication with similarly equipped users around the globe.

Electronic mail is useful because it permits the user to send a message to a friend or colleague even when the recipient is not available at his or her desk. When the recipient returns from lunch, from a meeting, or whatever, they will find the message in their electronic mailbox.

Electronic mail may also be useful in more of a real-time type conferencing situation where you will have multiple individuals that will use the electronic mail system as a substitute for a conference telephone call.

Unlike the postal mail where you send the letter and you may wait days for the recipient to receive it and be able to acknowledge it, with electronic mail that transaction can occur virtually instantaneously.

Additionally, of course, electronic mail messages may be sent not only to a single individual, but to a large number of predetermined recipients.

With the rapid proliferation of personal computers, communicating word processors and the like, it is easy to understand why the electronic mail industry is growing at a rapid rate.

Many analysts believe that the computer-based messaging industry is about $250 million of annual revenues today, but will grow to the $2 to $3 billion level in the early 1990's. There are currently several hundred million messages sent annually, and this figure will grow into the tens of billions in less than a decade.

It is reasonable to assume that during the next decade electronic mail will become a regular part of the communications mix that a substantial number of Americans use in the workplace and increasingly at home as well.

Mr. Chairman, with these comments as a preface to underscore the importance of this subject, let me say that we wish to commend you and Senator Leahy for developing this vitally important legislation.

We believe that S. 1667 deals with the key concerns regarding electronic mail privacy which warrant serious congressional attention. We were pleased to make recommendations to you and your staff during the drafting process for this bill.

During the 2 months since the bill was introduced, there has been a great deal of analysis and discussion of the legislation by various companies and industry associations in the field.

Given the complexity and importance of the subject matter, we believe it is quite encouraging that virtually all of the relevant players have expressed basic support for this legislation.

In large measure, the task at hand is to clearly delineate the intended sweep and coverage of the bill. As you know, the electronic communications field is quite diverse and rapidly changing.

One of the most significant aspects of this change is the increasing utilization of computer technology in telecommunications systems. The computer, in combination with conventional wire line and radio transmission media, can provide important new communications services and capabilities to users. Electronic mail is an excellent example of the marriage of these technologies.

In order to adequately protect the privacy of users of such computer-based electronic communications systems, legislation is needed which will cover electronic messages at all stages of their passage through an electronic communications system.

Thus, in an electronic mail system, a message must be protected while it is stored in the user's electronic mailbox located in the system operator's computer, as well as while it is being transmitted over telephone lines to and from the computer.

Indeed, protection of the message while stored in the computer mailbox is the most important aspect, for the message is most vulnerable to unauthorized access at this point in its passage through the overall communications system.

The need to protect the privacy of electronic communications while they are stored in a computer has given rise to questions concerning possible overlap between S. 1667 and the computer crime legislation which is currently being considered by the Laxalt and Hughes subcommittees.

We agree that clarification is needed as to where communications privacy concerns leave off and computer crime concerns begin. Some overlap between these two appears inevitable and is not necessarily undesirable.

The Electronic Mail Association recognizes the interrelationship of these two subjects and believes that both S. 1667 and a comprehensive computer crime bill are needed. Carefully crafted, these two types of legislation are essentially complementary to each other, for neither, standing alone, provides the full scope of protection which our industry needs.

Senator, we would like to compliment you and your staff for the very constructive undertaking that you have made here, and we would like to continue to work with you. I would like, in the interests of time, to skip over the remainder of my prepared statement.

But, essentially, we feel that the protections of the bill against unauthorized private interception are terribly important—both the criminal and the civil provisions. Additionally, we feel it is very important to have a clear standard that would apply in the case of Government access to electronic mail information.

At present, our industry does not believe that there is a clear standard governing governmental access and we feel that is needed as well.

Thank you.

[Mr. Walker's prepared statement follows:]

PREPARED STATEMENT OF PHILIP M. WALKER

ON BEHALF OF THE ELECTRONIC MAIL ASSOCIATION

Good morning, Mr. Chairman and members of the Subcommittee. I am Philip M. Walker, General Regulatory Counsel for GTE Telenet, Incorporated one of the nation's leading providers of packet switched telecommunications and electronic mail services. I am appearing today as Vice Chairman of the Electronic Mail Association.

The Electronic Mail Association is a Washington-based trade association created in 1983 by many of the leading companies in the field. The group now has over 60 members spread throughout the U.S. and Canada, and several European members as well. Our Board of Directors includes such companies as GTE, ITT, Western Union, MCI, IBM, Digital Equipment, and Citibank.

"Electronic mail" is a product -- an application -- of the melding of computer and communications technology. It allows virtually instantaneous communication with similarly equipped users around the globe. Electronic mail is useful because it permits a user to send a message to a friend or colleague even when the recipient is not available at his or her desk. When the recipient returns from a meeting, lunch, or whatever, they will find the message in their "electronic mailbox".

Also, a message, be it a few words like "the meeting is at noon", or a lengthy document stored in computer memory, can be sent to one recipient or literally hundreds of predetermined recipients, simply with the push of a button.

With the rapid proliferation of personal computers, communicating word processors, etc., it's easy to understand why the electronic mail industry is growing at a rapid rate.

Most industry analysts rate the computer based messaging industry as about a $250 million industry today, which will grow to the $2-3 billion level in the early 1990's. There are currently several hundred million messages sent annually, but this figure will grow into the tens of billions in less than a decade. It's reasonable to assume that, during the next decade, electronic mail will become a regular part of the communications mix that a substantial number of Americans use in the workplace, and increasingly at home as well.

Mr. Chairman, with those comments as a preface to underscore the importance of this subject, let me say on behalf of the Electronic Mail Association that we want to commend you and Senator Leahy for developing this vitally-important legislation. We believe that S.1667 deals with the key concerns regarding electronic mail privacy that warrant serious Congressional attention. We were pleased to make recommendations to you and your staff during the drafting process for this bill.

In the two months since this bill was introduced, there has been a great deal of analysis and discussion of the legislation by various companies and industry associations in the electronic communications field. Given the complexity and importance of the subject matter, we believe it is quite encouraging that virtually all of the relevant players have expressed basic support for this legislation. In large measure, the task at hand is to clearly delineate the intended sweep and coverage of the bill.

As you know, the electronic communications field is quite diverse, and rapidly changing. One of the most significant aspects of this change is the increasing utilization of computer technology in telecommunications systems. The computer, in combination with conventional wireline and radio transmission media, can provide important new communications services and capabilities to users. Electronic mail is an excellent example of the marriage of these two technologies.

In order to adequately protect the privacy of users of such computer-based electronic communications systems, legislation is needed which will cover electronic messages at all stages of their passage through an electronic communications system. Thus, in an electronic mail system, a message must be protected while it is stored in the user's electronic mailbox, in the system operator's computer, as well as while it is being transmitted over telephone lines to and from the computer. Indeed, protection of the message while stored in the computer mailbox is the most important, for the message is most vulnerable to unauthorized access at this point in its passage through the overall communications system.

The need to protect the privacy of electronic communications while they are stored in a computer has given rise to questions regarding possible overlap between S.1667 and the computer crime legislation which is currently being considered by the Laxalt and Hughes Subcommittees. We agree that clarification is needed as to where "communications privacy" concerns leave off and "computer crime" concerns begin. Some overlap appears inevitable, and not necessarily undesirable. The Electronic Mail Association recognizes the interrelationship of these two subjects, and believes that both S.1667 and a comprehensive computer crime bill are needed. Carefully drafted, these two types of legislation are essentially complementary to each other, for neither standing alone provides the full scope of protections which our industry needs.

With that in mind, we want to congratulate you, Senators Leahy and Mathias, and your staffs, for the very constructive beginning you have made. We look forward to working with you in the development of clarifying language, which will allay any concerns about the appropriate scope of your bill's coverage. Let me now comment briefly on a few of the principal elements of this legislation.

S.1667 goes to the heart of electronic mail privacy concerns by prohibiting unauthorized access to electronic communications systems. This is essential since, as I have mentioned, the most likely type of privacy invasion comes when an unauthorized individual attempts to enter the "electronic mailbox" of a system user. Messages are in place, awaiting properly authorized access by the boxholder. Just as letters sitting in conventional mailboxes at the curbside are afforded legal protection, we strongly believe that the public has a right to privacy for their electronic messages.

The bill provides a structure encompassing several different levels of civil and criminal penalties for privacy violations. We believe this differentiation makes sense, for it provides appropriately heavy penalties for cases of corporate espionage, while allowing lesser sanctions against the stereotypical young hacker. The bill does make it quite clear, however, that a youngster with a personal computer is committing a crime when he or she violates someone's privacy, just as if they stole the contents of somebody's conventional mailbox.

We also wholeheartedly endorse the concept of recovery of civil damages which is incorporated in S.1667. Citizens who have had their right of privacy violated should be able to sue the guilty parties. We see this as potentially an important deterrent as well.

The bill includes a provision which prohibits the employees of service providers from divulging the contents of any communication which they might inadvertently gain awareness of. We support this concept. It tracks similar provisions which have been in effect in the telephone and telegraph industries for decades. However, we are unclear at this time whether section 705 of the Communications Act, or your bill, would apply to the subpoena of electronic messages in certain civil lawsuits. This may simply be a matter of clarification which we will undertake to resolve with your staff.

S.1667 also includes legal mechanisms to regulate government access to electronic mail messages. We support these provisions, since at the present time companies in our industry are faced with no clear standards when government agencies seek access to subscriber information. This has not, as yet, become a common occurrence, but without Congressional action the uncertainty will continue. S.1667 establishes clear procedures, just as procedures currently are in existence for telephone wiretaps and surveillance of U.S. postal mail.

We also agree with the provision mandating that this legislation will cover any "provider of electronic communications service", not just communications common carriers. As you know, the Federal Communications Commission has defined electronic mail as an "enhanced service," not subject to common carrier regulation. Also, electronic mail systems are widely operated by corporations, non-profit organizations and government agencies for their own internal use. During the next decade these various discrete systems will increasingly interconnect with each other. Electronic mail users obviously deserve privacy protection regardless of what type of entity runs their system, or the system they reach a message recipient on.

In summary, the Electronic Mail Association believes that this is truly landmark legislation. In the coming months we believe that various definitional questions can be clarified, and we sincerely hope that final passage can be achieved during the present Congress.

Senator MATHIAS. Thank you very much.

Mr. Nugent.

STATEMENT OF P. MICHAEL NUGENT

Mr. NUGENT. Good morning, Mr. Chairman. My name is P. Michael Nugent. I am the government affairs counsel for Electronic Data Systems, which is a subsidiary of the General Motors Corp.

I am appearing today on behalf of ADAPSO. I am chairman of its Committee on Computer Systems and Communications Privacy and president of a section, which is the Network-Based Information Services Section.

Two hundred and fifty of ADAPSO's members are members of that section. They provide remote data processing services, electronic mail services, information management and distribution services, remote access to data bases.

In fact, one of ADAPSO's members offers a service called CHAT, which is an interactive electronic mail telephone conversation.

The other members of ADAPSO, including the members of the Network-Based Information Services Section, also want to thank you, Senator Mathias, for your work and that of this committee and that of the staff on other issues that are also important to us, such as the protection of computer software and other forms of computer software in terms of semiconductor chips, and so forth. We have been very grateful for your hard work.

We thank you for developing this necessary, this fundamental, this truly seminal legislation. It is necessary for the evolution of an information-based economy—that is, S. 1667.

The lack of the protections afforded by this bill will retard and impede the development and the public acceptance, we believe, of high communicating and processing technology. The protections in S. 1667 should, if they are broadly applied, prevent customers from losing their privacy rights when they resort, as they must in this day and age, to third-party processors and transmitters of data.

Or if these protections are not afforded, we may force customers to rely on less cost-effective and less efficient internal systems, because they are considered more private.

If I may, before getting into some of our comments about the substance of the bill, just touch on some of the Department of Justice comments about title III. The human voice, as I understand it, generates an analog signal or a sine wave that is carried over analog facilities.

Business machines and computers generate digital signals, on-off pulses, which represent information. Increasingly, voice is being digitized, and that voice-digitized transmission is being provided over cables, wires and radio transmission.

So we have an anomolous situation where the voice which is carried by analog facilities will be protected by title III. Yet, voice which is carried by digital facilities, whether they be terrestrial or satellite or other type, will not be protected.

And then you get the question raised by the testimony: Is title III really just protecting personal privacy or does it protect, as we always thought it did, the sanctity and the privacy of communications, per se. That is where we come in.

This bill grants privacy protection for data in transit, regardless of the technology used, be it microwave, satellite, wire line or fiber optic; regardless of the nature of the data in transit, be it voice image or information, personal, corporate, or institutional; and regardless of the regulatory status of the provider of electronic communications services, be it a common carrier or an unregulated provider of services.

In doing so, the bill updates the law to reflect how voice and information are conveyed today, and extends privacy protections for the electronic communications services that exist today and in the foreseeable future.

To fully protect the privacy and the sanctity of electronic communications, this bill wisely reaches beyond the mere transmission of the voice or the image or the information to that information, image or voice while it is being stored in connection with the provision of an electronic transmission or communication service. The bill does this with its unauthorized access and its disclosure provisions.

In doing so, the bill recognizes that privacy protection for an electronic communication is meaningless without complementary protection of the electronically communicated voice, image, or information while it is stored along the transmission path or in the computer communication systems at either the originating point of the communication or the terminating point of the communication.

ADAPSO is here, Mr. Chairman, seeking explicit clarification or expansion of the disclosure and access provisions of S. 1667, to realistically and fully apply these provisions to electronic communications as they exist today.

We are looking to see that electronic computer systems should be explicitly clarified or expanded to include all computer systems that are used by service vendors to transmit or process customer data which is electronically transmitted to such system, and explicit clarification or expansion of the bill's access and disclosure provisions to apply to electronically transmitted data not only while it is in transit to or from the service vendor's computer equipment—and we all use this computer equipment—but also while stored by the service vendor in connection with the service vendor's provision of data communications or remote data processing services.

Our customers should not lose their electronic communications privacy rights when they rely on third-party providers of data processing and data transmission services.

Another point to be raised is that the protections in this bill should, if broadly applied, prevent that loss of our business which will occur when we must shut down our computer system to search for records or data that the Government or a third-party litigant is looking for.

We are also looking for, Mr. Chairman, a clarification of whether the disclosure and access provisions of the bill are intended to prevent or limit service vendors from divulging electronically communicated information to nongovernmental parties in response to subpoenas in civil litigation. Right now, the law is, at best, unclear.

If this bill is not intended to so apply, we would be asking for third-party recordkeeping-type protections that are now in the Internal Revenue Code which provide for notice, standing, and the opportunity to object.

Mr. Chairman, we are going to be developing some schematic diagrams of two types of remote processing—remote access data processing and remote job entry. And we hope to be able to show with those diagrams where we think the electronic communication, so to speak, ends and where the storage unrelated to electronic communication begins.

I would ask permission to submit those separately under separate cover letter. I could get into them now, but I know you are interested in moving on.

Senator MATHIAS. We would very much like to have them.

Mr. NUGENT. Thank you.

Senator MATHIAS. If you will get them to us promptly, we can include them in the record, assuming they are appropriate for that purpose.

Mr. NUGENT. Thank you, Mr. Chairman.

[Submissions of Mr. Nugent follow:]

PREPARED STATEMENT OF P. MICHAEL NUGENT ON BEHALF OF ADAPSO

Mr. Chairman and Distinguished Members of the Subcommittee:

My name is Michael Nugent and I am the Government Affairs Counsel for Electronic Data Systems Corporation (EDS), a subsidiary of the General Motors Corporation. I am here today representing ADAPSO, the trade association for this nation's software and services industry. I serve as Chairman of ADAPSO's Committee on Computer Systems and Communications Privacy. I am also a member of the ADAPSO Board of Directors and have been elected President of the Network-Based Information Services Section.

ADAPSO welcomes this opportunity to address the Subcommittee on this vitally necessary legislation. At the outset, let me express ADAPSO's strong support for S. 1667. Members of ADAPSO's Privacy Committee have spent many hours working with staff on drafts of this legislation. Our support is subject only to the absolute need for clarification or expansion of certain premises and provisions embodied in the bill.

Before addressing the provisions of the bill, allow me to describe the business activities of the industry which ADAPSO represents.

The 250 member companies of ADAPSO's Network-Based Information Services Section operate remote access computer systems for the purpose of providing a wide variety of commercial computer-based services to their respective customers. Examples of these services include (1) electronic mail; (2) processing of service order applications; (3) remote access databases; (4) communicating word processors and work stations; (5) inquiry/response activities between customer terminals and central computer locations, such as status checks for airline flights or financial modeling applications; and (6) transactions such as electronic funds transfers. All of these services involve the electronic transmission of data between customer terminals and the vendor's computer system.

Data transmission capabilities also are used by the computer service industry to provide bulk data transfer applications. These applications include transfer of large data files between computers for processing and generation of desired functions (e.g., nightly transfer of billing data from remote locations to a central computer).

Many of the services that are performed by means of the transmission and processing of data might not commonly be thought of as electronic communications services, but they are functionally indistinguishable. Moreover, ADAPSO believes that information which is electronically transmitted to and from a service vendor's computer system in connection with the provision of commercial computer services should be entitled to communications privacy protection.

With this background, I would like to more specifically address a number of provisions of the Electronic Communications Privacy Act.

ADAPSO endorses and supports the concept of recognizing and protecting privacy interests in electronic data transmissions. We believe that there is a legitimate interest in the privacy of electronically communicated data. We also believe this is the same regardless of whether the data is transmitted for the purpose of receiving a communication service or a data processing service (assuming that it is possible to clearly distinguish between the two). Further, we believe that the term "electronic communication system" as used in Sections 102 (a) and (b) of the bill should be broadly defined to include all computer systems that are used by service vendors to transmit or process customer data which is electronically transmitted to such a system. These protections should apply to this data not only while it is in transit to or from the service vendor's computer equipment, but also while it is held by the service vendor.

The current language of the bill is rather ambiguous with respect to the terms "electronic computer system" and "electronic communication service". ADAPSO urges the Subcommittee to adopt a broad interpretation of these terms; an interpretation which include remote computing service systems in the term "electronic communication system," and remote computing services within the meaning of the term "electronic communication service."

Absent a broad interpretation of these terms, S. 1667 will beg the question of how to distinguish between information or data stored in an "electronic communications system" and information or data stored in a computer system that relies on data transmission to furnish services. ADAPSO is concerned that an overly narrow construction of the phrase "electronic communications systems" will frustrate the underlying purpose of Section 102. As Representative Kastenmeier has noted,

> "it would be inconsistent to prohibit the interception of . . . information in transit and leave unprotected . . . such information while it is being stored."

In addition to definitional problems, ADAPSO is concerned about the disclosure provisions of Section 102. First, be assured that the computer services industry has no interest in abusing the privacy rights of its customers. To the contrary, we are interested in ensuring strong privacy rights, because absent some assurance of privacy protection, our customers may be reluctant to use outside computer services. These same customers may instead establish more expensive internal systems, or for financial reasons, forego the tremendous benefits of computerization altogether. Only those companies who were large enough and financially able to afford to maintain and operate their own private networks will be able to protect their privacy interests. In order to encourage the continued development and use of innovative computer systems, strong privacy protection must be guaranteed.

Unfortunately, it is not clear whether the privacy protections created by Section 102(b) prohibit service vendors from divulging the contents of their customers' electronic communications to both governmental and non-governmental parties in both criminal and civil litigation. Our concern is that Section 102(b) is only intended to limit the ability of government agencies to require the disclosure of customer data in criminal proceedings. If no protection is created against subpoenas in civil litigation, ADAPSO believes that procedural safeguards similar to the third-party recordkeeper provisions contained in Internal Revenue Service Code Section 7609 (giving bank customers the right to receive notice of and standing to contest IRS subpoenas) would be appropriate.

ADAPSO also believes that it is essential for any federal electronic communications privacy bill to contain a preemption provision that would protect service providers from being subjected to conflicting state privacy protections. It would be manifestly unfair and impractical from a business standpoint to require service providers to segment their operations to comply with the different requirements of state statutes. Without a preemption provision, service providers would have to conform their operations to comply with the most stringent state law, which would then have the de facto effect of national law, superseding the carefully crafted balance of rights and duties in this bill.

Further, ADAPSO suggests that consideration be given to the following specific recommended language clarifications and corrections:

1. at page 2, lines 20 et seq.:

"(g) It shall not be unlawful under this chapter for any person —

"(i) to intercept an electronic communication made through an electronic communication system designed for the purpose of making an electronic communication readily accessible to the public.

2. at page 6, lines 1-8:

Substitute for the words "a user" the words "an authorized user". This change is necessary to prevent unauthorized users, who are nonetheless "users", from "authorizing" and thus legalizing improper access by one another. It will probably also be necessary to include a definition of the term "unauthorized user", which makes clear that such a user is a bona fide customer of the service provider in good standing, with respect to data assigned to a customer's file space.

3. at page 6, line 8:

After the word "while" add "it is in transit or".

4. at page 6, line 24:

Add after the word "communication" the words "from an authorized user." This change is necessary in order to ensure that legal privacy protection only applies to communications from authorized users. Hackers should not be subject to this type of protection; indeed, the contents of their communications often must be divulged--and removed from the system--in connection with routine service provider security investigations and enforcement activities.

5. at page 7, line 1:

Add after the word "addressee" the words "or intended recipient." This change is necessary because certain communications (e.g. communications to database providers on automated order forms) do not necessarily have an addressee.

6. at page 7, line 5:

   Add after the words "user originating such communication" the words "or the recipient." This change is necessary to permit recipients to authorize disclosure of the contents of communications sent to them. This type of disclosure may legitimately be required in connection with technical assistance activities, record retrieval, resolution of billing disputes, and security investigations.

7. at page 7, line 7:

   Omit the word "employed" and substitute instead "whose services or facilities are used." This will ensure that providers of service will be permitted to disclose when they assemble a network from different providers of transmission services or facilities.

8. at page 7, lines 9-12:

   The phrase "business activity" should be construed broadly enough so as to include activities related to the maintenance of the security of the electronic communications system. This is essential so that a provider of service may disclose an electronic communication to law enforcement authorities where the originator of such communication was not a customer of the electronic communications provider, but a hacker or other trespasser.

9. at page 8, line 9:

   The "and" in line 9 should be changed to "or" in order to protect from disclosure to the government not only a record kept by the provider in the course of providing that communication service, but also a record relating to any particular communication made through that service. This will protect not only records generated or created by the service provider, but also records supplied by the customer.

10. at page 8, line 22:

Delete the words "or used." This phrase is too broad and vague and does not relate to any substantive prohibitions.

CONCLUSION

ADAPSO applauds you, Mr. Chairman and your cosponsors for tackling what is a very complex, but important issue. The resolution of the issue of communications privacy is strategically important in the evolution of our information society and economy. You are updating the law to reflect the enormous changes prompted by technology , technology that has fundamentally changed how we communicate, what we communicate, and what we can do with the information. The computer software and computer services industry believes that S. 1667 is particularly timely legislation, because our customers need recognition and protection of their legitimate privacy interests.

In closing, I wish to make it clear that our support of electronic communications privacy legislation does not in any way diminish our support of computer crime legislation. We believe that in addition to legislation which recognizes and protects fully the privacy of electronic data communications, there is also a need to provide private sector computer systems with criminal law protection against unauthorized computer trespass. These are two separate issues, however, and both require a legislative remedy.

ADAPSO endorses S. 1667, and looks forward to continued involvement with you and your staff as this legislation evolves. We hope our comments will assist you in consideration of legislation that fully and realistically grants privacy protection to electronic communication.

EDS

Electronic Data Systems Corporation
Office of Government Affairs
1331 Pennsylvania Avenue, N.W.
North Office, Suite 1300
Washington, D.C. 20004
(202) 637-6700

October 8, 1986

The Honorable Charles McC. Mathias, Jr.
387 Russell Senate Office Building
Washington, DC 20510

Dear Senator Mathias:

You had allowed ADAPSO to supplement its testimony with respect to the workings of remote data processing services. Attached are two diagrams showing the flow of customer data when electronically communicated in connection with the provision of remote processing services.

There are basically two kinds of remote processing services--remote job entry and remote interactive processing. Diagram "A" deals with remote job entry and Diagram "B" sets out remote interactive processing.

Diagram "A"--Remote Job Entry

ADAPSO seeks expansion or clarification of the bill to protect data while transitting or being stored in the systems set out in the diagram, except for the following data or software stored in the system (items "5"):

1. Hard-copy documents generated at the customer site;
2. Operating software, application software, vendor or proprietary databases stored at the vendor's site; and
3. Archival records however stored (Archival records and vendor records regarding customer usage of vendor's service are, however, separately protected by the bill).

These three categories of data or software, as well as all other data stored on any computer system, should be the subject of computer crime legislation.

Some points of explanation need to be made: First, transmission between the customer's systems and the vendor's system should be distinguished from the "transmission" that is internal to a computer/communications system. Second, the "customer computer" (item "1") can be a PC, a minicomputer or a mainframe computer. Third, the "controller" (item "2") provides for memory or storage in connection with transmission; it provides an interface for remote communications; and also buffering which (in the transmission of data) consists of storage used to compensate for a difference in the rates of flows of data or for a difference in the time of occurence of certain events. Fourth, the "communications control" or "front-end processor" (item "2A") manages the data network and, through polling of data storage cites and through storage of data, controls the data flow between the network and the computer, permitting optimum operation of computer resources. The control also engages in certain processing of data both before and after applications processing. Fifth, the "online storage devices" at the customer and vendor locations (items "3") are used primarily to provide for temporary storage in the transmission of data for applications processing. The customer's online storage device (when used for "permanent' storage) and the vendor's "permanent" online storage device (item "4") are employed to retain online certain data for future transmission and applications processing. For example, these online "permanent" storage devices may be used for storage of data necessary, in the case of a depository institution customer, for generation of monthly statements and end-of-year reporting to tax authorities.

Diagram "B"--Remote Interactive Processing

ADAPSO seeks expansion or clarification of the bill to protect data while transitting or being stored in the systems set out in the diagram, except for the following data or software stored in the system (items "3"):

1. Operating software, applications software (unless customer provided);

2. Vendor or proprietary databases stored at the vendor's site.

These two categories of data or software (items "3"), as well as all other data stored on any computer system, should be the subject of computer crime legislation.

Some points of explanation should be made. First, the "customer computer" (item "1") is generally a PC or minicomputer, but may sometimes be a mainframe computer. Second, the points made previously about the "controller" (item "2") and transmission between customer and vendor versus "transmission" internal to a computer/communications system, also apply here. Third, when using a remote interactive computer service, a customer is provided the computer capability to create and/or store, maintain and process for itself the customer's own data (item "2A"). In fact, the customer is assigned its own "file space" within the vendor's computer. Customers use such remote interactive services to take advantage of the vendor's extensive network access to the customer's own data where the customer has a regional, national and/or international range of offices or locations. In addition, customers employ remote interactive services to take advantage of the computing power, sofware and data bases provided by the vendor.

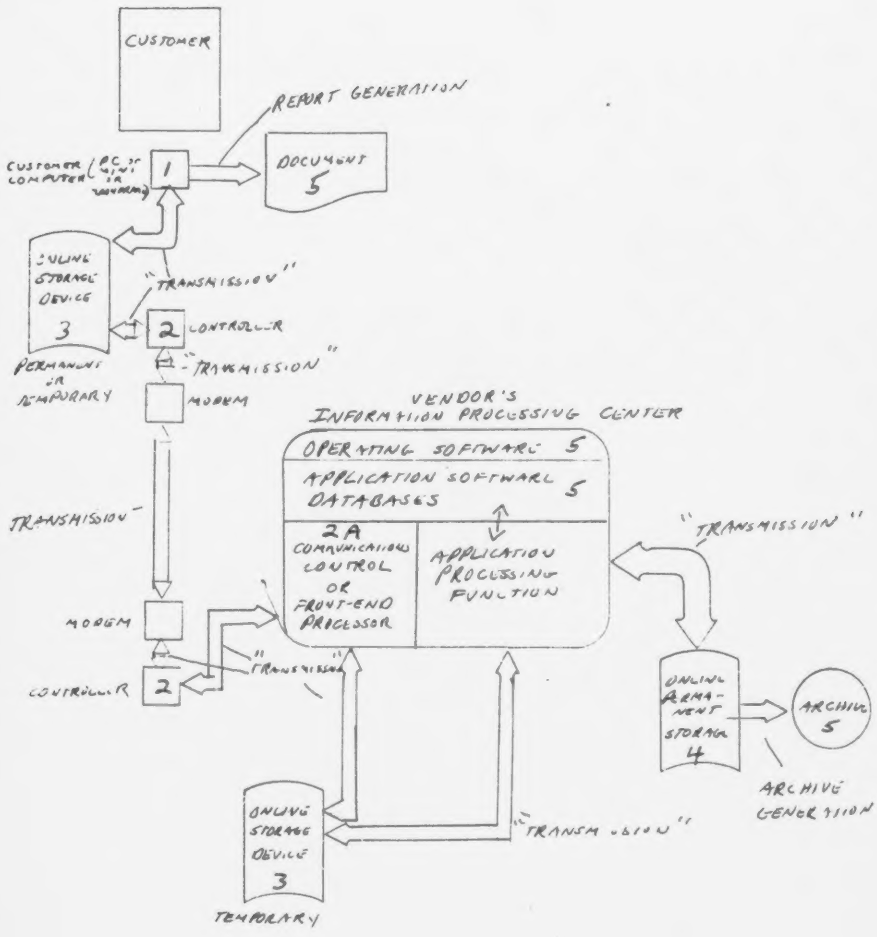
Sincerely,

Michael Nugent

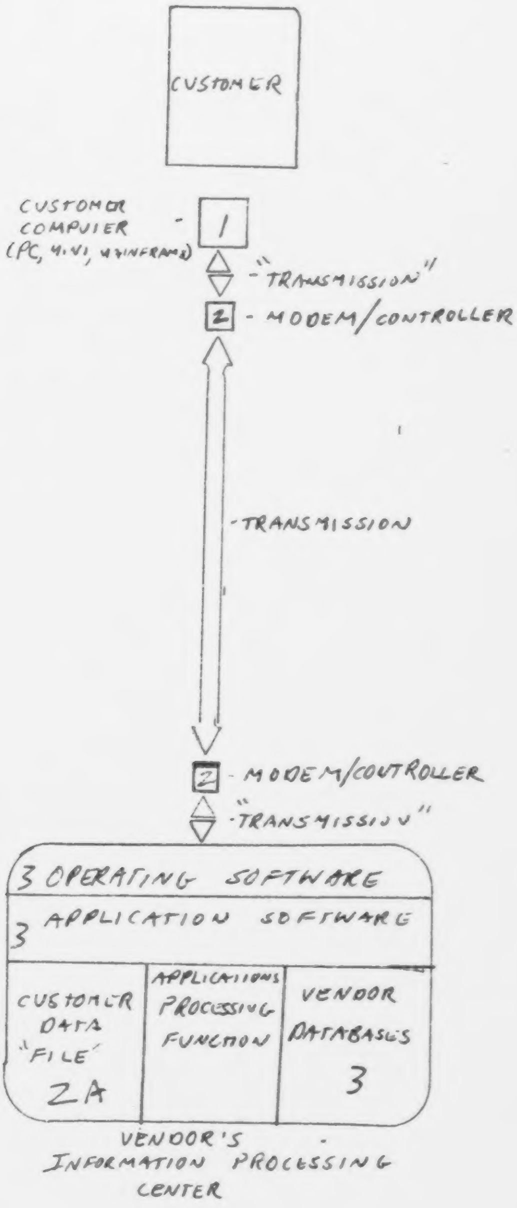
P. Michael Nugent

PMN/tap

A. REMOTE PROCESSING "JOB ENTRY"


CUSTOMER
REPORT GENERATION
CUSTOMER COMPUTER (PC or MINI or MAINFRAME)
1
DOCUMENT 5
ONLINE STORAGE DEVICE 3
PERMANENT OR TEMPORARY
"TRANSMISSION"
2 CONTROLLER
"TRANSMISSION"
MODEM
TRANSMISSION
MODEM
CONTROLLER 2
"TRANSMISSION"
VENDOR'S INFORMATION PROCESSING CENTER
OPERATING SOFTWARE 5
APPLICATION SOFTWARE DATABASES 5
2A COMMUNICATIONS CONTROL OR FRONT-END PROCESSOR
APPLICATION PROCESSING FUNCTION
"TRANSMISSION"
ONLINE PERMANENT STORAGE 4
ARCHIVE 5
ARCHIVE GENERATION
ONLINE STORAGE DEVICE 3
TEMPORARY
"TRANSMISSION"

B. REMOTE PROCESSING – "INTERACTIVE"


CUSTOMER
CUSTOMER COMPUTER (PC, MINI, MAINFRAME) - 1
"TRANSMISSION"
2 - MODEM/CONTROLLER
-TRANSMISSION
2 - MODEM/CONTROLLER
"TRANSMISSION"
3 OPERATING SOFTWARE
3 APPLICATION SOFTWARE
CUSTOMER DATA "FILE" 2A
APPLICATIONS PROCESSING FUNCTION
VENDOR DATABASES 3
VENDOR'S INFORMATION PROCESSING CENTER

Senator MATHIAS. Mr. Stanton.

STATEMENT OF JOHN STANTON

Mr. STANTON. Good morning, Mr. Chairman. My name is John Stanton. I have submitted separately written testimony and, in the interest of time, I am going to summarize my comments today.

I am executive vice president and chief operating officer of the Personal Communications Group of McCaw Communications. McCaw is a company providing service in the personal communications field to approximately 100,000 customers in 15 States and 35 markets. We are about the third largest company in the cellular business, about the seventh largest company in the paging business.

I am also chairman of Telocator. Telocator is the association of nontelephone company providers of cellular and paging services representing roughly 80 percent of the paging customers in the United States today.

Our industry serves roughly 5 million customers. Since 1968, it has grown twentyfold, from roughly a quarter million customers to the number I mentioned today. That has been a product of the change in the technology.

Twenty years ago, the size of a pager was much the size of a desk telephone. Things have changed radically. In 1968, 95 percent of the pagers being used only went "beep." Today, the technology has improved dramatically.

There are four kinds of pagers, those providing alpha-numeric, tone and voice, numeric, and the conventional tone-only pagers. In the cellular business, the most dramatic change has been the size of the equipment, changing from World War II when a radio had to be carried around on a backpack to today where it can conveniently be held in a customer's pocket.

The cellular telephone provides the convenience and expectation of a landline-quality telephone signal. If you have had an opportunity to use a cellular telephone, the quality of the service in this area and in most areas of the country today would deny the receiver of a communication being originated by a cellular caller of knowing whether or not that communication was coming from a wireline telephone or a cellular telephone.

The four kinds of pagers I mentioned have changed radically as well. Twenty years ago, the tone-only pagers were roughly this size [indicating]. Today, a pager can be as small as a pen. This digital display pager provides services so that I can receive a numeric message. They are also available with alpha-numeric messages so that I can conveniently receive messages anywhere in the country.

The users of our medium have changed as well. Today, many businessmen, lawyers, doctors, government officials will have pagers and paging equipment, as well as cellular equipment.

In 1968 when the Omnibus Crime Control and Safe Streets Act was passed, my industry almost did not exist. My industry certainly did not need privacy protection at the time when pagers only went beep.

Today, we provide service equivalent to a telephone company, and yet the protection of the wiretap legislation of 1968 is not extended to our industry. The technology that allows our industry to have grown dramatically also allows interception, so that our customers are denied the benefits of privacy that their wireline colleagues are allowed.

The quality of transmission is the key in terms of the preservation of the expectation of privacy. If I called you on this telephone, the conversation would not be protected, and yet you would have no idea that the call was being transmitted in part by radio waves.

Transmissions can be intercepted, and are on a daily basis. Electronic "peeping toms" are stealing business secrets and overhearing advice between lawyers and their clients, doctors and their patients, denying people the right of privacy.

The creation of the complex and invisible web that you spoke of in your introductory statement has integrated different kinds of communications so that electronic mail, cellular communications, and paging, as well as conventional wire, are all part of the same network and all deserving of the same kind of protection.

Cellular represents a new, improved technology, an alternative to being out of touch and an alternative to expensive new telephone poles and wires. Today, in many cases, telephone companies are considering the possibility of building cellular communications as an alternative to building conventional systems, so that in rural areas telephone service will be provided less expensively, but it will not be afforded the privacy unless this legislation passes.

My industry will bring service to the public. All we are asking is that our customers be afforded privacy. We believe that the Electronic Communications Privacy Act is a crucial piece of legislation which would afford us that privacy.

We have addressed with staff certain technical issues which we think can improve the bill, but fundamentally we support it.

Thank you.

[The prepared statement of Mr. Stanton follows:]

PREPARED STATEMENT OF JOHN STANTON

ON BEHALF OF TELOCATOR NETWORK OF AMERICA

Good morning, Mr. Chairman and members of the Committee. My name is John Stanton. I want to thank you for providing me with the opportunity to testify with regard to S. 1667, the Electronic Communications Privacy Act of 1985. I am the Executive Vice President of McCaw Communications Companies, Inc., which provides mobile communications services in many parts of the United States.

This morning, I am testifying on behalf of Telocator Network of America. Telocator is the national association of non-telephone company radio common carriers (RCCs) which provide cellular telephone, two-way radio and paging services to the public.

Telocator does not represent and does not include within the scope of these remarks, the Private Land Mobile Services, regulated under Part 90, Title 47 of the U.S. Code. Private services are provided only to those involved in some type of business or governmental enterprise, while public services are operated by radio common carriers who are required to provide services to all citizens on a nondiscriminatory basis.

According to several recent studies, public demand for paging and cellular radio services is increasing at a rapid pace. Arthur D. Little, Inc., an investment research firm, projects that there will be 10 million pagers in service in the United States by 1990 and that the industry will grow about 2.5 times in the next five years, for a compounded growth rate, in terms of subscribers in place, of more than 20 percent.

Similarly, market studies of the cellular industry predict that there will be 2.5 to 4 million subscribers to cellular radiotelephone service by 1990.

Cellular radio is an important new innovation in mobile radio technology. The idea was first developed by engineers at Bell Labs in the 1950's and the needed computer and switching technologies became available in the 1960's. The key development was a system which "reused" frequency spectrum through a technique of dividing the service area into "cells". As vehicles and other mobile users move from one cell to another they move within range of a different switching station, enabling a new user to make use of a channel in a cell which has just been vacated. Instead of using a single transmitter to cover an entire city, a cellular system divides up a city into several hexagonal cells.

Radio common carrier or paging services involve either the use of radio signals for communications between two or more fixed (base) radio stations or the use of such signals for communications between fixed (base) radio stations and individuals or moving vehicles. Most RCCs offer paging service as well as traditional two-way mobile service.

Cellular and modern paging telecommunications services are products of the technology revolution that is still underway. Significant changes have taken place in personal communications services -- changes that were not foreseen in 1968 when the Omnibus Crime Control and Safe Streets Act was passed. That federal act, which would be amended by S. 1667, severely limits the circumstances in which an individual's telephone conversation can be intercepted or disclosed. It was passed at a time when telephone conversations were almost exclusively transmitted over wire, from one stationary telephone to another, and pagers were primarily limited to emitting a "beep" tone only[1]. The amount of mobile two-way radio service then was small because the technology was inadequate and few radio channels were allocated for such service. Congress, therefore, designed its statutory protection mainly for the privacy of the traditional telephone conversation.

---

[1] Voice and tone pagers represented 5% or less of paging in the U.S. at that time.

Since then, technology has advanced and hundreds of new channels have been made available for cellular mobile communications to meet the demands of a highly mobile population. Today's sophisticated paging systems are capable of sending alphanumeric messages of 80 or more characters, and similar systems are expected, in the near future, to have the capacity to transmit considerably longer messages. In addition, the Federal Communications Commission (FCC) last year adopted procedures governing the licensing and use of radio frequencies to provide nationwide network paging2.

Thus, technology has provided us with entirely new modes of communications. Yet, recent State Supreme Court decisions have held that communications received over radio are not "wire communications" within the meaning of Title III of the Omnibus Crime Control and Safe Streets Act[3], thereby denying privacy protection to one of the fastest growing segments of the communications industry. These judicial decisions are based on the technology involved--radio technology was not accorded a reasonable expectation of privacy because the technology made it easy to eavesdrop. However, the general public does not distinguish between a telephone conversation transmitted by wire or by radio in terms of privacy. The right of privacy is a funda- mental right irrespective of the means by which the message is carried.

It is, therefore, incumbent upon Congress not to alter certain privacy expectations, but to develop legislative guidelines so that national policy may keep pace with

---

2 A network paging system would enable a subscriber to receive pages when traveling outside the local service area.

[3] Rhode Island v. Delaurier, 488 A.2d 688 (R.I. 1985)

technological advancement. Failure to modernize the privacy statute to account for new technologies and services could discourage use of mobile communications services, thereby stifling emerging industries and limiting the benefits of enhanced mobility of telecommunications to the public.

The Federal Communications Commission (FCC) also expressed its concern about the privacy issue last year in the Nationwide Paging Service proceeding as follows:

> ...we would like to express our concern about the privacy of subscribers using alphanumeric paging equipment....these systems are vulnerable to interception by undesired third parties and the messages conveyed are easy to store and sort with computers. This can pose a threat to the privacy of subscribers. While we do not have a record at this point on which to propose a specific action, we would like to point out to the operators of all sophisticated paging systems our concern in this area...

For these reasons, Telocator Network of America supports the need for legislation such as S. 1667. The Electronic Communications Privacy Act would provide the crucial legal protection necessary to prevent unauthorized access or interception of electronic communications, including cellular telephony and paging. It would bring the United States Criminal Code up to date with the electronic revolution and establish criteria so that privacy protection can catch up with technology.

While Telocator heartily supports the broadening of Title III privacy protection to include electronic communications, several provisions in the legislation, as introduced, may be cause for concern. For example, S. 1667 would exempt from privacy protection communication systems that are "readil accessible to the public". Because over-the-air radio transmissions can be intercepted, this somewhat vague exception from protection could be construed to cover, for example, cellular communications which the legislation is otherwise intended to protect.

Also, the bill prohibits the _installation_ or _use_ of "tracking devices" without a court order. Telocator suggests clarification of the definition of "tracking devices" and/or the installation provision so as not to impede the installation or use of paging and cellular telephone equipment.

Telocator believes that these provisions can be easily clarified without impairing the basic purpose of the legislation and we are ready to work with the Subcommittee and staff in crafting any necessary modifications to the bill.

In summary, Telocator Network of America strongly endorses the expansion of privacy protection to electronic communications as embodied in S. 1667 and we would like to thank Senators Leahy and Mathias for their continued efforts toward this end.

Thank you for allowing me the opportunity to testify this morning. I will be happy to answer questions at this time.

Senator **Mathias**. Thank you very much, Mr. Stanton.

Let me ask you all this question. Is privacy important to your business? Mr. Walker gave us some statistics on his projections in this whole field. Enormous growth is anticipated in the industry. So we are talking about a substantial new industry coming on line in America.

Is privacy important to it? Do you have any evidence on which to base an opinion that customers are concerned about that issue?

Mr. **Walker**. Well, Senator, if I could begin to answer that question, the electronic mail industry provides a substitute, an alternative, and we believe oftentimes a more efficient form of communication, in place of either voice telephone calls or use of the regular mail system.

Oftentimes, because of the rapid transmission capability of electronic mail and the interactive capability that it affords, it will primarily substitute for voice telephone. Now, the individual making a voice telephone call is afforded statutory protections and protections that have proven to be extremely important to individuals transmitting sensitive information over the telephone; that is, communicating by voice.

If those individuals are to be able effectively to embrace this new technology as a substitute, then they need to have a comparable level of protection.

With respect to the Justice Department's statement this morning where it was suggested that electronic mail is nothing more than a substitute for postal mail, I would have two comments.

First, that is not entirely accurate. As I say, I think often it is more a substitute for the telephone. But, second, with respect to even postal mail, there are statutory provisions that bar private citizens from intercepting the U.S. mail. There are criminal penalties for interception of the U.S mail.

There are no comparable penalties with respect to the interception of electronic mail. Even with respect to Government access to electronic messages, it is not entirely clear to us in all cases that a search warrant under the Federal Rules of Criminal Procedure would be involved.

It may be the practice of the FBI to obtain such search warrants, but in a State law enforcement investigation I am not sure that that would be the case. And our industry feels that the service providers do not have a clear standard as to what their obligation is to disclose that information.

By the same token, the user does not have the assurance that his information in the hands of the service provider will be protected. So I think that the bottom line of all that is that it inhibits people's ability to utilize this new technology.

To that extent, it retards not only the growth of our industry, but the productivity of the entire economy.

Senator **Mathias**. Your last comment is a pertinent one for this committee. You believe it inhibits the growth of the industry. I assume that you other gentlemen would agree with that.

Mr. **Stanton**. Mr. Chairman, I can speak specifically to that. Our industry has grown based on an expectation of privacy. Many of the ads that different competitors within the cellular communications industry have used, have used the words "private communications" or "private line" because that is what contrasts our service to the traditional mobile telephone services that had been offered to subscribers.

However, in some cases our communications are not private because of the recent developments in the scanner technology that is beginning to retard the usage among certain segments.

We are going to take certain steps to provide better security for customers who can afford to pay it. Encryption is an example, but encryption is not a substitute for this legislation, nor is the legislation a substitute for encryption. Both are necessary.

What we need is a national understanding and a national policy, if you will, for privacy that would affect our customers, because it will otherwise retard our business.

Mr. **Nugent**. Mr. Chairman, if I could just chime in here, this matter is really an Achilles heel of the information services industry generally. Our customers come to us because they cannot meet their own internal data processing-data transmission needs.

In turn, they have got to turn their data over to us; in other words, let it outside their doors. If the customers were to perceive that they were less protected when they went outside, then we would lose business. It would be very much a cramp in the growth of the business.

This arises in the context of not only interception, but Government access to data that we hold. Who should control that data? Also, third-party access—the issue becomes, does the customer still have rights and standing to object when an improper subpoena or motion to disclose comes to the provider of service?

So there are very real questions in our industry when we hold the customer's data about third-party access in the course of civil litigation, and also Government access. Who owns the data? What standing does the customer have? Should the customer have standing? There are issues like that that are fundamental to the growth of this industry.

Senator MATHIAS. Is that more or less what you meant, Mr. Walker, when you said that the industry is faced with no clear standards when Government agencies seek access to subscriber information?

Mr. WALKER. Well, the standing question is one element of that, even with respect to the service provider itself. My company, for example, provides an electronic mail service. In doing that, we maintain a computer system that has electronic mailboxes of hundreds of thousands of users, each of which may contain messages to or from the holder of that mailbox.

Now, if we are faced with a Government request for access to certain of those messages, what standard applies? If the FBI comes to us, I gather that they would first obtain a search warrant under rule 41.

But if it is a State or a local law enforcement agency, it is not clear that a comparable procedure would be followed. That puts the service provider in the predicament of wishing on the one hand to protect the privacy of his users, but on the other hand being subjected to requests which have the color of authority which he may feel obliged to respond to.

It is a difficult situation that we feel we and our customers should not be put into. We feel that there should be a clear, uniform standard that applies to any requests for production of this information.

Senator MATHIAS. You have described the electronic mailboxes as the most vulnerable part of the system. Why is that the most vulnerable part of the system?

Mr. WALKER. Well, electronic mail consists of three steps. First, the message is transmitted over, normally, conventional telephone lines to the electronic mailbox. Then it is stored in the mailbox, waiting for the recipient to pick it up. Finally, it is transmitted from the mailbox to the recipient.

Those two transmissions may be intercepted in the conventional fashion. A wiretap can physically be placed on a telephone line. The information is digital, but it can easily be read out on a computer if it is attached to that telephone line.

However, it is difficult, in practice, for a private citizen to accomplish such an interception. The Government would have no difficulty doing it, but a private citizen would.

On the other hand, once the information is in the computer mailbox, someone may attempt to penetrate the computer. For example, each user of the computer system, the electronic mail system, is given a password which he has to enter in order to have access to his mailbox.

If another individual somehow gains knowledge of that password, he may be able to then impersonate the authorized box-holder and enter the system and access the contents of the mailbox.

That, in practice, may be a far easier task for him to accomplish than physically wiretapping the target's telephone line. So, in practice, we have found in the industry that the kind of problems we have had with unauthorized intrusions have occurred in somebody coming into the computer mailbox rather than somebody physically wiretapping the telephone line.

Senator MATHIAS. What about the question I raised with the Justice Department on the description in a search warrant that would identify the message in the computer mailbox?

Mr. WALKER. Well, I am not a criminal lawyer and I am not familiar with the detailed procedures that one would have to go through in order to get a search warrant. But oftentimes there will be a whole variety of messages dealing with different topics in a user's mailbox.

There may be an interactive process, as I mentioned in my testimony, in some systems where it is almost like a conference telephone call.

Senator MATHIAS. Message and reply.

Mr. WALKER. Messages and replies from multiple parties; it is not necessarily just a two-way conversation, so that you would have a whole community of users who are communicating about a topic through their respective mailboxes, with copies of messages sent from one recipient to all the others, and then a reply from one of the others back to all of the set.

So to try to identify a particular message in that context might be difficult, and I really do not know how the courts would deal with that in terms of granting a search warrant.

But we, as service providers, would not be able to easily differentiate those messages. We feel that they are all private and we wish to protect the privacy of the system users. Yet, as I say, we are put into this dilemma if presented with a request from a law enforcement agency.

Senator MATHIAS. Mr. Nugent, you referred to the fact that we ought to protect not only the messages in transit, but also at what you have called the data base. Is that essentially the same concern Mr. Walker has expressed about the electronic mailbox?

Mr. NUGENT. It is essentially the same, Mr. Chairman. This is a continuing problem. What kind of storage do we want to protect under the rubric of communications privacy? We have been grappling with that over the past many months.

It seems to us that the kind of data that should be protected is not so much data bases that reside in a computer system per se, but rather customer data which is transmitted back and forth for the purpose, in our industry, of processing and transmission services.

A good example is, for instance, in the bank context we do data processing for banks. We have storage points all along in our remote job entry type of processing service where we store literally at four or five points along the transmission path and in the computer itself.

All of this storage, however, is for the purpose of further transmission and for the purpose of getting into the computer. In other words, our software that resides in our computer tells the storage device when to send the data to the computer for processing. So there are many applications to that.

There is also the interactive context—and I think this is more applicable to what Phil just said—where, if you can envision a mailbox type of system in a post office and you walk in and you see a hundred of them, the customer will send their data into one of those mailboxes.

He does that in an interactive context because his computer is too small; he has got an international client base that cannot be served by his own facilities. The customer data is stored in that little mailbox and the customer has access on demand to get in and out and manipulate that data, and also to reach into the other mailboxes and use software and data bases that reside in those other mailboxes.

So what we are saying is that the customer-submitted data, the data that has been submitted to the vendor for the purpose of processing and transmission, is the data that should be protected, not the data bases that one would think normally just reside on a computer system for the purposes of providing a service other than in the customer context.

So I think we are talking about essentially the same thing, which is the customer uses communications to get a data processing or data transmission service.

Senator MATHIAS. Mr. Stanton, you mentioned paging devices. In the old days when you had an early page boy or whatever they called them—bell boy——

Mr. STANTON. Bell boy.

Senator MATHIAS [continuing]. Bell boy. You got a beep, and really all that beep told you was go to the telephone and call your office. When you called your office, you might be told aurally to call 456-1414.

Now, that aural communication by telephone would be protected under the views expressed by the Justice Department today. Why should there be a difference in the protection accorded today's device? If you hear the beep, go to the telephone and are advised to call 456-1414, why should that be more protected than if you get a direct transmission of the telephone number 456-1414?

Mr. STANTON. The easy answer is that all of those kinds of communications should be afforded equal protection. If I may, Mr. Chairman, take one small step back and describe the differences among those pagers, it may overcome a misunderstanding or misconception, I think, that underlies some of Justice's comments.

Fundamentally, the difference between the kind of paging service that we may provide in different markets is based on the frequencies on which we provide the service. The four different kinds of paging services that I mentioned—a tone and voice pager that may look like this, a digital display pager that may look like this, the bell boy pager that you described before, or a tone alert or alpha-numeric display pager—all receive signals that are sent over the same frequency.

The 158.7 megahertz frequency, which is P-6, to which this pager is tuned, for example, could send any kind of communication. So the notion of interferring or receiving or illegally intercepting a communication over that frequency would enable the interceptor to receive messages of all types, including the ones that they wanted to receive and any others.

So from my point of view, the notion of saying that they can wiretap a tone-only pager but they cannot wiretap an alpha-numeric or a tone and voice pager is based on a misunderstanding of my business.

Fundamentally, they are going to intercept the signals to this pager; they will get the signals going to this pager as well. That absence of difference, if you will, requires the uniform protection of all of the services because if you agree that the tone and voice pager should be protected, then because the same frequencies provide all kinds of services, you must extend the same protections, really, to all of those services.

Senator **Mathias**. Thank you very much, Mr. Stanton.

Unfortunately, there is another rollcall vote in the Senate, so we will have to suspend this panel at this time. When I return, we will take the next and last panel.

[A brief recess was taken.]

Senator **Mathias**. Gentlemen, I am sorry you have been delayed. As you know all too well, that is the nature of our existence. It falls to you to make some sense of everything that has been said this morning, so if you would let us have your statements, then we can discuss the subject a little bit.

STATEMENT OF A PANEL, CONSISTING OF JERRY J. BERMAN, CHIEF LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON, DC, AND LYNN W. ELLIS, CHAIRMAN, COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, WASHINGTON, DC, ACCOMPANIED BY P. HOWARD PATRICK

Mr. **Berman**. Thank you, Senator. I am Jerry Berman, with the American Civil Liberties Union. First of all, I want to commend you, Mr. Chairman, Senator Leahy, and Representatives Kastenmeier and Moorhead for developing and then introducing this far-reaching legislation.

In our view, it is the most significant congressional privacy initiative since the Privacy Act of 1974, and we strongly support its overall objectives.

The principal aim of S. 1667 is to protect the privacy of new forms of electronic communications. It recognizes that we are in the midst of a technological revolution in the way we communicate private messages; that new forms of data communication such as electronic mail are augmenting or taking the place of first-class mail and telephone conversations; that wire, microwave, cellular, radio, and other transmission means are carrying voice, text and video message images separately and in combination; and that many of these messages are being handled not only by common carriers, but by new private communications systems.

I think the push for this legislation—and I think it is a broadly formed coalition of interests—comes from the now widely held view that the case law and statutory law is simply out of date and it is ineffective in protecting communications carried by new technologies.

We would just underscore our appreciation that you are "calling in your chips" with the Attorney General on this legislation. Leaving the Senate, you leave a gigantic note for civil liberties protections. This would be a major monument to your work in the Congress.

Many things are at stake here. First of all, on the one hand, I think the productivity and growth of whole new technologies and industries which could be adversely affected—on the other hand is citizens' privacy.

Without this legislation, left to the courts and left to the Justice Department's changing interpretation of what the law is, a myriad of lawsuits could result in the near future. It is just an event waiting to happen and it could drastically adversely affect privacy and new technologies.

The Justice Department today added to the confusion which they have helped to generate over the last 1½ years. They have taken a number of contrary positions, first saying that new communications were protected under title III, but on a case-by-case basis, then saying maybe it was protected by the Foreign Intelligence Surveillance Act, or maybe both.

Now they argue, it is not under title III, but under rule 41 search warrant procedures. A year ago in a case in Michigan, they argued that there was no protection whatsoever for electronic mail. They were simply records like bank records which had no privacy protection and the Government could cease them with a bareface subpoena.

So the Justice Department has been all over the map, and I think that an additional chip you now have is that they owe it to the country to help you clarify the law in this area.

I want to make three points that come out of our study at this area of law. Over the last 1½ years, the ACLU has conducted a privacy and technology project and we have brought together on two separate occasions a wide range of business groups, privacy interests, and technology experts to look at this very issue.

Those consultations were widely attended by business, industry, public interest, and business organizations, and three major conclusions were reached. The first is that title III does not protect many of the new forms of communications; that it protects against government and private interception of aural communications, but not data communications. It certainly does not cover cellular telephone communications, and it certainly does not cover non-common-carrier companies.

In the face of our current communications revolution, the law is simply out of date.

The second conclusion of these consultations was that title III should protect the contents of private electronic communications against government and private interception, regardless of its form or means of communication.

As a matter of privacy rights, it should not make a difference whether a person communicates with another party by having a phone conversation or sends the same message in text over a phone line using a computer, a modem, and an electronic mail service; nor should it make a difference whether a communication is carried by wire, microwave, or cellular phone service.

The Justice Department today seemed to make some distinction, or tried to make a distinction, between data communications like electronic mail and telephone communications.

One, they argue that phone communications are more private. That is just not the history of the fourth amendment. The fourth amendment only covers telephone conversations since 1967.

Senator **Mathias**. There were no telephones when the fourth amendment was written.

Mr. **Berman**. There were no telephones, but when there were it took 40 years for the courts to recognize interception of conversations as a trespass. So if you start from that analogy, the mail deserves more protection under the fourth amendment than telephone conversations.

But the analogy breaks down because this is a mixed medium of communications; we do not even have a clear legal language to talk about it. It looks like mail at one point, but then it could be—streams of data communications, two-way conversations, teleconferencing, financial records being sent back and forth, funds being transferred across data lines between companies and between two points and two parties.

So, how the Government can use a rule 41 warrant to even particularize a search in this area is beyond my imagination. When they said that to move this into title III would move thousands of cases over, I think you really need to ask them what they are talking about.

Where do the thousands of cases involving data communication come from? We looked for them as examples and there are very few. How do they get them confused in this way? I do not think they can use rule 41, at least while data is in the stream of communication.

There, it ought to be brought under title III, and it makes absolutely no sense to distinguish between private interception and government interception for purposes of privacy protection, or to separate them out into different statutes.

They raise the same fundamental issues; it is just the contents of private communications being sent by different media and new ways, in text, in video, in voice, and sometimes mixed together.

Third, and most important, the conclusion of our consultations was that if privacy protection was going to make any sense at all, you have to protect the messages when they are being held for forwarding by new industries like electronic mail companies.

They are intermediaries between the sender and recipient of messages, and it is that point in the transaction where the messages are most vulnerable. Since these companies, for auditing and customer convenience, create backup copies of those records, you need to protect those records after the transaction or the message has been forwarded to the ultimate addressee.

The reason for that technically is that because of the changes in fiber optic cables and new technologies, it is difficult to intercept streams of communications and to wiretap the new forms of data communications. It is not impossible, but difficult.

If you want to get access to this electronic mail, you go down to the electronic mail company and you seize it. Now, the Justice Department said that this would require a rule 41 search warrant; that in their view at this stage of the transaction you might be able to particularize and you might be able to meet rule 41 standards.

But it should be recognized that the Justice Department is here allowing a higher standard than the sponsors of this legislation have put in the bill for taking records, and it is a fundamental change from the Justice Department's position in 1982 when they argued in court that private records of electronic mail communication held by an electronic mail company in Michigan were not protected under any privacy law and they could be seized with a bareface subpoena; that they were just records really owned by the electronic mail company. So this is a major change toward privacy protection, and I think you ought to hold them to that standard.

To try and summarize, I think that S. 1667 addresses all three of these fundamental points raised in our consultations. One, it protects data and voice communications; it protects them whether they are carried by common carrier or noncommon carrier. It protects cellular radio.

It requires a warrant for government intrusion and it makes it a crime for private, unauthorized access to those messages.

Third, it protects the messages when they are held for storage and forwarding by creating criminal penalties and civil liability. So it addresses the major gaps in current law and we are very much in support of this legislation and anxious to help to refine it. There are many terms which need to be defined in the legislation, but it is moving in a direction which I think is a fundamental change in the law which is necessary to protect both privacy and other interests.

Finally, there is a second section of the bill which is an attempt and a second principal thrust of the legislation to update title III and our current law to establish some minimum standards for pen registers, tracking devices, and other new technologies of investigation.

As I have followed this, we have long supported establishing minimum standards for pen registers and tracking devices. We think they rise to a level of intrusion which should establish the need for court scrutiny and some minimum standard of relevance to law enforcement before government can seize these records.

As I have followed the debate over what these standards should be, our sense is that these standards in this bill essentially codify current practice and should not be an enormous burden to the Justice Department.

I think Representative Kastenmeier, who is principally responsible for trying to legislate in this area, has accommodated the Justice Department in many of these areas. And now their testimony opposing these sections today is inexplicable. They are attacking proposed rules which essentially incorporate their own practice.

It seems to me that since the courts in the fourth amendment area are constantly making a havoc of the lines between what is legal and illegal under the fourth amendment—a beeper is not a violation of the fourth amendment up to your front door if it is on you, but if you go through the door, it violates the fourth amendment—that the government should welcome some certainty and clarity in this area.

From a civil liberties point of view, some minimum standards are called for. So I think that both aims of the legislation are accommodated here. The legislation deserves support and we are anxious to work with you to enact this legislation, hopefully in this session of Congress.

[Mr. Berman's prepared statement follows:]

PREPARED STATEMENT OF JERRY J. BERMAN

ON BEHALF OF

THE AMERICAN CIVIL LIBERTIES UNION

Mr. Chairman and Members of the Subcommittee:

Introduction

On behalf of the American Civil Liberties Union, I want to thank you for requesting our testimony on S. 1667, the Electronic Communications Privacy Act of 1985. As you know, the American Civil Liberties Union is a nonpartisan organization of over 250, 000 members dedicated to the defense and enhancement of civil liberties guaranteed by the Bill of Rights.

We want to take this opportunity to commend the Chairman, Senator Patrick Leahy and Representatives Robert Kastenmeier and Carlos Moorhead on the House side for developing and introducing this legislation. In our view, it is the most significant congressional privacy initiative since the Privacy Act of 1974 and we strongly support its objectives. Over the coming months, we are anxious to assist the sponsors and other members of the Congress to perfect this legislation and work for its passage.

In our testimony today, we want to state our general understanding of what this far reaching legislation seeks to accomplish and why we endorse those objectives. Our concerns about the legislation are cautionary. If enacted, S.1667 will regulate new technologies of communication which are complex and evolving. Every effort must be made to insure that the legislation protects the privacy of new electronic communications without unintentionally stifling technical or social innovation or inhibiting the free flow of information. Congress, the public, and affected industries must work to craft the legislation to avoid any adverse unintended consequences which might result from regulating new communication technologies and enterprises.

Protecting the Privacy of New Forms of Communications: The Need for New Law

The principal aim of S. 1667 is to protect the privacy of new forms of electronic communications. It recognizes that over the last decade new technologies have brought about fundamental changes in the ways we communicate private messages. New forms of computer driven "data" communications such as electronic mail services are augmenting or taking the place of telephonic voice communications and traditional mail sent through the postal system. Wire, microwave, cellular radio and other transmission means are carrying voice, text, and video messages and images separately and in combination. Such messages are being handled not only by common carriers but by new private communications systems.

The push for legislation arises from the now widely held view that case law and statute have not kept pace with communications innovations and afford little if any legal protection against unauthorized government or private interception of new electronic communications. For example, this is the principal conclusion of the Office of Technology Assessment's recently issued study on Electronic Surveillance and Civil Liberties.

In this regard, the American Civil Liberties Union's Project on Privacy and Technology, which I direct, has held two major consultations over the past year and a half with privacy and technology experts, business and public interest groups to explore the legal status of new forms of communication. For your deliberations, I ask that the Summaries of these two consultations be made a part of the record. Briefly, let me state the consultation findings which parallel those of the Office of Technology Assessment:

First, the principal statute, Title III of the Crime Control and Safestreets Act of 1968, only prohibits unauthorized government or private interception of "aural" communications carried in part by wire over common carrier systems. In the face of our current communications revolution, the law is sadly out of date.

Second, the law should protect the "contents" of private communications regardless of its form or means of communication. As a matter of law, it should not make a difference whether a person communicates with another party by having a phone conversation or sends the same message in text over a phone line using a computer, a modem, and an electronic mail service. Nor should it make a difference whether a communication is carried by wire, microwave, or cellular phone service.

Third, and most important, legal protection for new forms of communication will be illusory if Congress only protects communications privacy while messages are being transmitted over common carrier networks. Electronic mail, for example, is sent to an electronic mail company and placed in an "electronic mail box" for later delivery in electronic or hard copy form to the addressee. For auditing and customer convenience, a record copy of a message is held by the electronic mail company after the message is delivered. Both from a technical and legal perspective, new electronic communications are most vulnerable to unauthorized interception while they are being held for forwarding or recorded for backup purposes. Technically, it is easier to intercept a message here than when it is in the stream of communication. Legally, a message is most vulnerable because of legal precedents holding that citizens have no privacy rights in sensitive records held by third parties. e.g. United States v. Miller, 425 U.S. 435 (1976).

S. 1667 and Electronic Communications

S. 1667 would amend Title III to afford privacy protection to new forms of electronic communication. It would amend Title III's definition of "interception" to prohibit the unauthorized interception of private data and voice communications however transmitted. Government investigative agencies would need a judicial warrant based on probable cause to intercept "data" communications carried by wire, microwave, or other means, and voice communications transmitted by cellular radio. Communications would be protected even if carried by non-common carriers. A private party would violate privacy rights by intentionally intercepting such communications without consent. Violators would also be subject to civil liability.

S. 1667 would also protect "records" of communication held by providers of electronic communications services such as electronic mail companies by making it a crime for any person to gain unauthorized access and obtain or alter such records and by making service providers subject to civil liability if they divulge such records. The government must obtain a Title III warrant or court order based on reasonable suspicion to search and seize such records.

We strongly endorse this legislation. As we said at the outset, our concerns are cautionary. By defining "electronic communication" broadly and by leaving undefined such key concepts as "electronic communications systems", "electronic communication service", "a provider of an electronic communication service", and "authorized access", the bill is subject to a myriad of interpretations as to the scope of what is intended to be or what is in effect protected by its provisions.

At this point, the focus should be on the appropriate policy objectives rather than the exact meaning of the bill's provisions. We support the legislative intent to protect the privacy of "data" and other new forms of non-public electronic communications while they are being transmitted from one party to another and the contents of those communications when they are held by third party companies for forwarding to an addressee and any record backup of such communications stored or retained by third party intermediaries.

We recognize that there are a number of other data security issues which may need to be addressed by federal law. The issue is whether they should be addressed in a bill designed to protect communications privacy. We think not. However, we also know that drawing the line between public bulletin boards and private networks is difficult. Similarly, it is an open question whether a data base of information created by one party and held by a communications service for later distribution to customers should be an electronic communication within the meaning of this bill or a data base requiring protection under a federal computer crime statute. Likewise, protecting internal corporate and government communications systems, however desirable, poses complicated problems of distinguishing communications systems from other internal computer data bases for purposes of protecting private messages and insuring that employees, particularly government employees, are not unduly inhibited from divulging information otherwise available to the public. The central task now is to sort these issues out.

S. 1667 and Electronic Surveillance

Another principal aim of S. 1667 is to clarify the warrant requirements of Title III and establish minimum safeguards for the investigatory use of new electronic surveillance techniques such as pen registers and tracking devices. Of course, we strongly endorse this objective.

The ACLU has long held that the minimization requirements under Title III will remain ineffective until Congress sets new guidelines for the courts. We view the information generated by pen registers as sensitive enough to require the government to meet some minimum standards of relevance before obtaining such records. Recently the courts have begun to recognize that modern tracking devices are intrusive in some circumstances and that today's surveillance technology is too sophisticated to sustain judicial precedents which analogize electronic tracking to traditional physical surveillance. United States v. Karo, 104 S. Ct. 3296 (1984).

Since the government has interpreted the criminal penalties of The Foreign Intelligence Surveillance Act to require a court order for pen registers and since the courts have begun to set Fourth Amendment limits on tracking devices, we view the proposed changes as serving the interests of civil liberties and law enforcement. The statutory amendments would give law enforcement guidance and certainty and create minimum standards and accountability mechanisms which protect civil liberties. Having studied the Justice Department's response to last year's bill introduced by Representative Kastenmeier, we believe the legislation essentially codifies current administrative practice and should pose no serious problems for law enforcement. These amendments deserve broad congressional support.

Conclusion

In conclusion, we strongly support the effort to protect the privacy of new electronic communications and establish minimum privacy safeguards for the investigative use of new surveillance technologies. We believe that the Congress is the appropriate body to deal with the complexity of new technologies and develop appropriate legislative guidelines which balance investigative needs and protection of civil liberties.

As you know, Title III was a response to the 1967 Katz decision which held---after forty years---that wiretapping violated the Fourth Amendment. Society cannot wait another forty years for the courts to catch up with the new technology or trust they will devise rationale rules by deciding on a case by case basis issues which affect complex, interrelated technologies and social arrangements. For those who decry judicial activism in fashioning protection for individual rights, this legislation affords an opportunity to demonstrate that Congress as well as the courts can be a guarantor of civil liberties.

Again, we applaud the sponsors for undertaking to develop and introduce this significant legislation. We are anxious to work with the Congress to refine its provisions and hope that it can be passed in this session.

Senator MATHIAS. Thank you, Mr. Berman.

Dr. Ellis.

STATEMENT OF LYNN W. ELLIS

Dr. ELLIS. Mr. Chairman, my name is Lynn W. Ellis. I am chairman of the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers.

This organization is the world's largest engineering society, with nearly 260,000 members worldwide, 214,000 of whom live and work in the United States. My committee is vested within the IEEE with authority to develop the institute's communication and information policy. Once that policy is adopted, our committee is one of the major mechanisms by which the policy is voiced to the public.

We thank you for the opportunity to present our views on S. 1667, the Electronic Communications Privacy Act of 1985. Our committee has endorsed this in principle, and we support measures to protect against the unauthorized interception and access in communications and computer systems.

We support, in particular, the attempt of the bill to extend the protections against the interception of voice transmission to virtually all electronic communications. The present hole in the wiretap law of not applying its protection to other than voice communications will be eliminated.

Our comments address mainly the technical issues that arise from the definitions and provisions of S. 1667. We especially wish to eliminate technologically restrictive language which may limit the provisions of the act in the years to come, as has happened with the current wiretap law.

We have no comment at all on the procedural requirements to be followed by law enforcement and the judiciary, as discussed by previous speakers.

Our comments are divided into two parts. The first part identifies the issues that were raised when our committee discussed S. 1667, and the second part of my comments, which I will not discuss today but have been submitted for the record, details our proposed changes in the wording of S. 1667 and the reasons for those changes.

The following are the issues I wish to address: the definition of the term "electronic communication," the definition of the word "intercept," lack of a definition of the word "access" and other terms in S. 1667, exceptions with respect to electronic communications, and the title of S. 1667.

The proposal of replacing the phrase "wire communications" with the phrase "electronic communications" in a new definition is a bold step in the right direction. The problem of trying to apply the outdated term "wire communications" to modern technology is eliminated, and I believe this addresses the specific examples raised by Senator Leahy this morning.

In the proposed definition for electronic communications, we have a few suggestions. We feel the word "photoelectric" has a specific connotation in physics and should be replaced by the more inclusive term "photoelectronic." This will avoid the confusion of whether fiber optics is or is not a type of medium subject to wire communication rules.

A second problem arises because of the inclusion of radio transmissions, the interception of which is also covered by section 705, previously named section 605 of the Communications Act of 1934. We ask how will the jurisdiction of each act be delineated in the proposed legislation to avoid contradictory results?

The phrase "any transmission," we believe, should be expanded to "any communication made in whole or part through the use of facilities for the transmission." We believe in this case that the protection belongs with the facilities, not the communications content

The expectation of privacy language should be added at the end of the definition.

In definitions of the word "intercept," we have two suggestions. We recommend that the word "intercept" be stricken, and that the "plain meaning" control, as in section 705 of the Communications Act because the definition is circular.

"Intercept is the interception of" would seem to require that the plain meaning of the word "interception" will control, despite inclusion of "intercept" in the definitions. Or if the word "intercept" is to have a definition, we recommend that the word "interception" be replaced by "unauthorized acquisition," so that the meaning is not circular.

The language "or other technological means of interception" should be added to the end of the definition to prepare it for the evolution of technology with time.

S. 1667 does not have a definition for the word "access," and for a number of other terms. In the second part of these comments, we have provided a proposed definition for "access" and would be glad to work with your staff in working out proper definitions of the other terms that are not so defined.

In discussing this in our committee, we had a problem with the term "readily accessible" in section 2511(2)(g). "Readily accessible" and "accessible" do not seem to us to have any distinction. Something is accessible or it is not; there is no practical use of the modifier "readily."

In the interests of keeping the language such that it would handle the technological changes of the future, we feel the term "walkie-talkie" is technologically restrictive and should not be continued as a specific term, so that there will be a broader applicability as technology changes.

Finally, we had some trouble in discussing the title. We recommend that the title be changed to "Electronic Surveillance Act of 1985." The issue here is perceptions and semantics rather than technology.

The most widely quoted definition of privacy is probably Alan Westin's:

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about themselves is communicated to others.

We find that S. 1667, as presently drafted, does not provide controls over when, how, and to what extent information is communicated. Rather, it seeks to provide protections to the electronic communication systems so that when a communication is made, there will not be any unauthorized interception.

The bill, as currently drafted, appears to us to control communications systems, not the communications contained within the systems.

Mr Chairman, I thank you for your attention to our statement. I have with me Dr. Howard Patrick, a member of the committee, to assist in case there are any technical clarifications you may wish us to handle.

[Dr. Ellis' submissions for the record follow:]

PREPARED STATEMENT OF DR. LYNN W. ELLIS

ON BEHALF OF THE COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY OF THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

Mr. Chairman, my name is Lynn W. Ellis, Chairman of the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers (IEEE). The IEEE is the world's largest engineering society, with nearly 260,000 members worldwide, 214,000 of whom live and work in the United States. Approximately 82% of our membership is employed in industry, 8% in academic institutions, and 10% in the various government laboratories and agencies. The IEEE Committee on Communications and Information Policy is vested with authority to develop the Institute's communications and information policy; and, once that policy is adopted by the Institute, our committee is one of the major mechanisms by which the policy is voiced in public.

We thank you for the opportunity to present our views on S. 1667, the "Electronic Communications Privacy Act of 1985." Our Committee endorses S. 1667 in principle. We support measures to protect against the unauthorized interception and access of communications in communications and computer systems. We support, in particular, the attempt of S. 1667 to extend the protections against the interception of voice transmission to virtually all electronic communications. The present hole in the Wiretap Law of not applying its protections to digital information will be filled.

Our comments address mainly the technical issues that arise from the the definitions and provisions of S. 1667. We especially wish to eliminate technologically restrictive language, which may limit the application of the provisions of the Act in the years to come, as has happened with the current Wiretap Law. We have no comment on the procedural requirements to be followed by law enforcement and the judiciary, to authorize the use of electronic surveillance techniques, such as wiretaps, pen registers, and tracking devices.

Our comments are divided into two parts. The first part identifies the issues that were raised when our Committee discussed S. 1667. The second part of the comments, which I will not discuss today, but will submit for the record, detail our proposed changes in wording of S. 1667, and the reasons for those changes.

Following are the issues I wish to address:

1. Definition of the term "Electronic Communication"
2. Definition of the word "Intercept"
3. Lack of a definition for the word "Access" and other terms in S. 1667
4. Exceptions with respect to electronic communications
5. The title of S. 1667

1. Definition of the Term "Electronic Communication"

The proposal of replacing the phrase "wire communication" and its definition, with the phrase "electronic communication" and a new definition, is a bold step in the right direction. The problem of trying to apply the outdated term "wire communication" to modern technology is eliminated.

However, in the proposed definition for "electronic communication:"

- The word "photoelectric" should be replaced by "photoelectronic"
- A problem arises because of the inclusion of radio transmissions, the interception of which are also covered by Section 705 (previously numbered Section 605) of the *Communications Act of 1934.* How will the jurisdiction of each act be delineated to avoid contradictory results?
- The phrase "any transmission" should be expanded to "any communication made in whole or part through the use of facilities for the transmission"
- The "expectation of privacy" language "where the person originating such communication exhibits an expectation that such communication is not subject to interception under circumstances justifying such expectation" should be added at the end of the definition.

2. Definition of the Word "Intercept"

We recommend that the definition of the word "intercept" be stricken, and that the "plain meaning" control, as in Section 705 of the *Communications Act*.

The proposed definition is circular, "intercept is the interception of..." and would seem to require that the plain meaning of the word "interception" will control.

If the word "intercept" is to have a definition, we recommend that:

- The word "interception" be replaced by "unauthorized acquisition"
- That the language "or other technological means of interception" be added to the end of the definition

3. Lack of Definition for the Word "Access" and Other Terms in S. 1667

S. 1667 does not have a definition for the word "Access." In the second part of these comments we have submitted a proposed definition for the word.

Other terms which need definitions are "Electronic Communication Systems," "Electronic Communication Services," "Provider of Electronic Communication Services," and "User of Electronic Communication Services."

4. Exceptions With Respect to Electronic Communications

In the proposed Section 2511(2)(g):

- The term "readily accessible" should be changed to "accessible."
- The term "walkie-talkie" should be deleted.

5. Title of S. 1667

We recommend that the title of S. 1667 be changed to the "Electronic Surveillance Act of 1985." The issue here is perceptions and semantics rather than technology.

The most widely quoted recent definition of privacy is probably Alan Westin's: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others."

S. 1667 does not provide controls over "when, how, and to what extent information ... is communicated." Rather, it seeks to provide protections to the electronic communications systems so that when a communication is made, there will not be any unauthorized interception. S. 1667 attempts to control the communication systems, not the communications contained within the systems.

Mr. Chairman, thank you for your attention to our statement. I will be happy to address any questions that you or the Members may have.

Proposed Changes in Wording of S. 1667
and
Reasons for Changing

Sec. 101 FEDERAL PENALTIES FOR THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS

1. Definition of the Term "Electronic Communication"

The proposed definition is as follows:

"'electronic communication' means any transmission of signs, signals, writing, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, or photoelectric system that affects interstate or foreign commerce."

a. "Photoelectronic System" Rather Than "Photoelectric System"

Recommended additional language:

"'electronic communication' means any transmission of signs, signals, writing, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, or ~~photoelectric~~ photoelectronic system that affects interstate or foreign commerce." (Underscore indicates language to be added, strikeover indicates language to be deleted.)

In physics, the word "photoelectric" refers narrowly to the ejection of an electron from a solid by an incident photon. The word "photoelectronic" refers to the combining of the technologies of optics and electronics, which is the intention of the definition.

b. Inclusion of Radio Transmissions Within the Definition of "Electronic Communication"

Since the definition of the term "electronic communication" includes radio transmissions, the interception of which are also covered by Section 705 (previously numbered Section 605) of the Communications Act, how will the jurisdiction of each act be delineated to avoid contradictory results?

For example, the Communications Act requires that the intercepted radio communication be also divulged and published; Section 2511(1)(a) of the Wiretap Law as amended by this Act only requires that the electronic communication be intercepted.

c. Addition of Language from Current Wiretap Law Definition of "Wire Communication" (Sec. 2510 (1))

Recommended additional language:

"'electronic communication' means any communication made in whole or in part through the use of facilities for the transmission of signs, signals, writing, images, sounds, data or intelligence of any nature ~~in whole or in part~~ by a wire, radio, electromagnetic, or [photoelectric] [photoelectronic] system that affects interstate or foreign commerce." (underscore indicates language to be added, strikeover indicates language to be deleted.)

The additional language is more consistent with the current defintion of wire communication; this means that judicial interpretations applied to the earlier definition may be more easily used as precedent for the new definition. The additional language, however, in no ways limits the more varied forms of communication that the new definition is intended to encompass.

Including the phrase "use of facilities" emphasizes that the protections are applying to the communications systems rather than the communications contained within the system, stressing the fact that the means of communication and not the content are being regulated. This helps to avoid potential conflicts between the 1st Amendment rights for free speech and trying to regulate (and possibly having to monitor) communications.

d. Addition of Language from Current Wiretap Law Definition of "Oral Communication" (Sec. 2510(2))

"'electronic communication' means any [communication made in whole or part through the use of facilities for the] transmission of signs, signals, writing, images, sounds, data or intelligence of any nature [in whole or in part] by wire, radio, electromagnetic or [photoelectric] [photoelectronic] system that affects interstate or foreign commerce where the person originating such communication exhibits an expectation that such communication is not subject to interception under circumstances justifying such expectations." (Underscore indicates language to be added.)

The expectation of privacy language added at the end of the definition is consistent with the language currently employed in the definition of "oral communication" in Section 2510(2) and U.S. Supreme Court decisions on privacy issues. If it is to be excluded, it is critical that the legislative history provide some rationale as to why:

- The "reasonable expectation of privacy test" is not to be applied to "electronic communications," but is to be applied to "oral communications."

- "Electronic communications" are to have absolute protection, unless subject to one of the stipulated exceptions.

2. Definition of the Word "Intercept"

The proposed amendments to the current definition are as follows:

"'intercept' means the ~~aural acquisition~~ interception of the contents of any ~~wire~~ electronic or oral communication through the use of any electronic, mechanical, or other device." (Strikeover indicates language to be deleted, underscore indicates language to be added.)

Our recommendation is that the definition of the word "intercept" be deleted, and that the "plain meaning" control, as in Section 705 of the Communications Act. The proposed definition would seem to require that the "plain meaning" of the word "interception" will control.

If the word "intercept" is to have a definition, we would recommend that in the proposed definition the word "interception" be changed to "unauthorized acquisition," and that additional language be added to avoid limiting the interception to "through the use of any electronic, mechanical, or other device."

> "'intercept means the ~~interception~~ unauthorized acquisition of the contents of any electronic or oral communication through the use of any electronic, mechanical, or other device or other technological means of interception." (Strikeover indicates language to be deleted, underscore indicates language to be added.)

3. Lack of Definitions for the Terms "Access," "Electronic Communication Systems," "Electronic Communication Services," "Provider of Electronic Communication Services," and "User of Electronic Communication Services"

S. 1667 does not contain any definitions for the above terms. At this time, we would like to propose the following definition for the word "access":

> "'access' means to instruct, interact or communicate with, intercept, or otherwise make use of any resources of an electronic communication system."

4. Exceptions With Respect to Electronic Communications

a. Proposed Section 2511(2)(g)(i)

> "(g) It shall not be unlawful under this chapter for any person--
>
> (i) to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public."

What does "readily accessible" mean? What would be the difference between "readily accessible" and "accessible"?

b. Proposed Section 2511(2)(g)(ii)(II)

> "(g) It shall not be unlawful under this chapter for any person--
>
> .
> .
>
> (ii) to intercept any electronic communication which is transmitted--
>
> .
> .
>
> (II) by walkie-talkie, or a police or fire communication system readily accessible to the public.

Same problem with "readily accessible" as described in "a." above. The term "walkie-talkie" is a layman's term, is technologically restrictive, is covered by the proposed Section 2512(2)(g)(i) ("an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public"), and can be deleted.

SECTION 1. SHORT TITLE

5. Proposal to Change Title of Act from "Electronic Communications Privacy Act of 1985" to "Electronic Surveillance Act of 1985"

For the reasons given below, we recommend changing the title to "Electronic Surveillance Act of 1985."

- The term "Electronic Surveillance" rather than "Electronic Communications Privacy" is more representative of the issues addressed in the provisions of this Act and the Wiretap Law, which it amends.

- The major purpose of the provisions is to regulate the circumstances under which government agencies may conduct electronic surveillance upon electronic communications systems.

- Privacy is not the main thrust. The most widely quoted recent definition of privacy is probably Alan Westin's: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

The provisions of this Act do not provide controls over "when, how, and to what extent information... is communicated." Rather, it seeks to provide protections to the electronic communications systems so that when a communication is made, there will not be any unauthorized interception. This Act attempts to control the communication systems, not the communications contained within the systems.

Note: an advantage of emphasizing the providing of protections to the electronic communications systems rather than the communications contained within the systems, is that it avoids potential conflicts between the 1st Amendment rights for free speech and trying to regulate (and possible having to monitor) communications.

Senator MATHIAS. Well, let me ask you this question from a commonsense point of view, but also from the point of view of engineers; I hope there is no difference. The law today distinguishes between a voice transmission and a data transmission. It distinguishes between communications carried by a common carrier and those that are not carried by a common carrier.

It distinguishes between communications that travel in part by wire and those that do not. You heard the Justice Department testimony on the digital telephone.

In the first instance, the law would seem to prohibit interception, but in the second case permit it. Now, is this common sense, or is there any engineering justification for these kinds of distinctions?

Dr. ELLIS. There seems to me to be a very limited engineering justification for these distinctions. The intent of the communication is to be made in private form, except with certain classes of communications where a specific warning has been included in the licensing of these communications, such as cordless telephones where the manufacturers are required to put a statement on the container that communications are not expected to be private under the terms of licensing of the communications.

Apart from that, the distinctions between radio and wire communications are rapidly blurring. The distinctions between message mode—that is, voice, visual, data or character—are rapidly blurring.

We felt in discussing this act that extending the spirit of the legislation to all forms of electronic communications, other than those where there is a specific reason why privacy may not be expected, would be an appropriate way to go.

Senator **Mathias**. Let's assume the Senate buys a digital telephone system, but the messages are carried by wire to someplace several blocks away and at that point they go wireless. The Justice Department says that system would be protected.

But how is anyone to know whether the message travels by wire or radio? What sort of notice are people under? Mr. Berman, do you want to take that?

Mr. **Berman**. Yes. I think what the Justice Department is saying is that the distinction in title III is not between aural and digitized signals--analog and digitized. The distinction is between aural communications and data communications.

They would say that aural communications, even if carried in analog and then converted into digitized form over long telephone lines, would not change the result under title III. They would go and get a title III warrant.

What they are saying is that the result changes if what is being communicated is data communications or nonaural communications. Then title III does not apply, and for some reason they are hemming and hawing about extending the protection to those communications under title III when, in fact, there should be no distinction.

Senator **Mathias**. So the transmission of a text or an image would not be protected under their approach.

Mr. **Berman**. Under their definition, they say it will be protected because they will go to court and get a rule 41 search warrant. But I think that is going to be very difficult for them to use.

I would like to see some examples of how they structure their application for a warrant in those circumstances. It is very interesting that Judge Posner, in the seventh circuit in the *Torres* case dealing with video surveillance, held that video surveillance is not under title III. He did turn to rule 41 and fashioned a search warrant and said you need a search warrant for such surveillance. He then urged the Congress to move this new technology into title III because it is complex, it is interrelated.

We are dealing with ISDN where we have voice, text and video all traveling the same stream, and the judge said Congress ought to rationalize these and put them in title III, and I think that is where they ought to go.

The Justice Department cannot—if they begin to focus in on what they are saying and understand the technology, they will not hold to their current position and will instead embrace the spirit of title III.

Dr. **Ellis**. Mr. Chairman, I believe there are two different sets of distinctions in what we have. One is the distinction between aural and nonaural communications, and the video, character and data are all not covered because of the specific limitation to aural and they should be covered, which your legislation addresses.

The second distinction is between the outmoded term "wire communications" and newer forms of communications, such as radio communications on the one hand, which was discussed well today, and also what I have called photoelectronic communications over optical fibers.

I do not believe that a technical witness would agree that an optical fiber is wire communications in the plain language sense of the meaning of "wire." So there is a need to cover the variations in message mode and the variations in technology with inclusive definitions.

Senator **Mathias**. Now, Mr. Berman, you have raised an interesting point that in our effort to protect privacy, particularly the confidentiality of computer data bases, we ought not to restrict public access to government information which would otherwise be available to the public.

Do you think that our efforts to assure privacy of communications present a difficulty in this case?

Mr. **Berman**. Well, I think that certainly the intent of the sponsors of this legislation, having sponsored legislation to overturn a statute that last year did essentially that in the name of computer crime, is not to do that.

And I think that all of the organizations that we have talked to who are supporting the legislation do not want to see that happen either. But I think a strained reading of the legislation, particularly because of the absence of certain definitions, can lead you to that interpretation.

Therefore, in our extended testimony we say that if we have concerns about the legislation, they are simply cautionary. All of us are dealing here with new technology, interrelated, complex, and we have to be careful in scrubbing this legislation down and refining it to see that we do not have any of these unintended consequences.

For example, the legislation would not only cover external communications system, for example, where citizens use the MCI or an electronic mail service to send messages in data form across the country, but internal corporate and governmental communications systems.

That is a desirable goal, but in refining the legislation it must be clear that the prohibitions against divulging information communicated through internal systems is not a new statute, making it a crime to divulge information otherwise available to the public; for example, an internal communication system between HEW and Agriculture, and you send a message between those two agencies and then say it is still in that stream of communication or is being held like electronic mail and therefore you cannot divulge it.

I think it is not explicit in the statute, but an employee might have a potential chill. But since that is not the intent of the drafters, the real task is to ensure, in refining the language of the statute and defining some of its terms and in legislative history, that that certainly is not the intent, and it only reaches communications that are intended to be private.

Senator **Mathias**. Let me ask you a subjective question. Do you think there is any difference whatever in the expectation of privacy between someone who uses a cellular phone and the traditional phone?

Mr. **Berman**. You know, "expectation of privacy" is one of the slipperiest terms ever developed by the court because you can defeat expectations of privacy simply by saying, well, we now have the technology for listening to telephone conversations without tapping them; we just can do that.

In fact, some of our agencies, I think, can do that. So where is the expectation of privacy? You no longer have it. You can go that direction, and cellular radio, because it happens to be able to be picked up unintentionally on radio band, poses that problem.

So you could say since it can be picked up, you should not have an expectation of privacy. But if Congress wants to create an expectation of privacy, then I think you are making a policy judgment and saying we are going to draw the line and give you that expectation of privacy.

Senator MATHIAS. What about digitized computer communications of text or an image? Is there an expectation of privacy there?

Mr. BERMAN. When I send our legislative strategy from our office on this piece of legislation to our executive director in New York using my computer and a modem to a computer in New York and it says, here are the following 12 amendments and here is what we should give up on, we certainly intend and expect that to be a private message and not covered by a rule 41 search warrant or by a record statute or a Government subpoena, but that there is a title III warrant to intercept that communication.

Dr. ELLIS. Mr. Chairman, I would say that in general there is an expectation of privacy except where the user of one of these technologies has been warned that privacy is not intended.

I would say the warnings, for example, on cordless telephones are so clear that there should not be an expectation of privacy in that case. There are a number of other examples where information is put on various radio frequencies for various general purpose uses which fall in that general category.

But for the user of a computer message system of any sort, not just electronic mail, I believe there is an expectation of privacy.

Senator MATHIAS. I would agree with that. I can go back to my Navy days. We used to have a radio system called TBS, talk between ships. You knew when you communicated on TBS that every ship that was within range was going to pick up your communication. There was no expectation of privacy.

Similarly, if you use a telephone from an airplane, or even a telephone from a car, usually one or the other party begins by saying we are communicating by radio telephone and it is not secure, and so you immediately shatter the expectation of privacy.

But without those kinds of rather positive signals, I think there is generally an expectation of privacy.

Mr. BERMAN. For example, you can read cordless phones out of this legislation, but the person with the cordless phone knows that he has a phone which may be picked up on someone's radio at the pool at the house next door. But the person with whom he is communicating does not know and does have an expectation of privacy.

Senator MATHIAS. And unless the caller from the airplane or from the cordless phone tells you this is a radio communication and it may not be secure, you have the expectation of privacy.

Mr. BERMAN. And I certainly think that what the electronic mail industry was saying this morning and other industry representatives is that they do not want to put on their product, this is mail, but it does not have——

Senator MATHIAS. Warning, warning.

Mr. **Berman** [continuing]. Warning: It is not protected under current law or it is not secure.

Senator **Mathias**. Do not say any thing you do not want to see in the papers.

Mr. **Berman**. Then its marketability as a product, you know, diminishes. So there is a nice convergence here between economic interests and privacy civil liberties interests.

Senator **Mathias**. Well, maybe that is a good point on which to end the hearing. But let me first thank each of you for having stuck with us until the end. I apologize again for the fact that we had several delays in the course of the hearing which have postponed us to the point that it has now invaded your lunch hour.

Mr. **Berman**. Thank you very much, Senator.

Senator **Mathias**. The subcommittee will stand in recess, subject to the call of the Chair.

[Whereupon, at 1:03 p.m., the subcommittee was adjourned.]

APPENDIX

DOCUMENTS REFLECTING DEVELOPMENTS ON THE ELECTRONIC COMMUNICATIONS PRIVACY ACT SUBSEQUENT TO THE HEARING ON S. 1667

STATEMENT OF SENATOR CHARLES McC. MATHIAS, JR.

SUBCOMMITTEE ON PATENTS COPYRIGHTS AND TRADEMARKS

MARK-UP SESSION ON S. 2575

AUGUST 12, 1986

Today the Subcommittee on Patents, Copyrights and Trademarks considers an important bill to enhance the privacy of Americans and update the provisions the 1968 wiretap act. The Electronic Communications Privacy Act of 1986, S. 2575 is identical to H.R. 4952 which passed the House Judiciary Committee by a vote of 34-0. That bill was approved by the House by a voice vote.

Subcommittee members are already familiar with the basic outlines of this legislation, since we held hearings last fall on an earlier version of it. In essence, the Electronic Communications Privacy Act responds to new developments in computer and communications technology by amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968 -- the federal wiretap law -- to protect against the unauthorized interception of electronic communications. Currently, Title III covers only voice communications. The bill expands coverage of the wiretap act to include data and video communications on nearly the same basis as conventional telephone technology. In addition, the bill eliminates the distinction between common carrier communications and private carrier communications. S. 2575 extends privacy protection to new forms of electronic communications, but is careful to exempt media in which privacy is not expected, such as tone only paging devices; amateur radio services; police, fire, and other public safety radio communications systems; and many satellite transmissions, including network feeds destined for rebroadcast, and satellite cable programming as defined in section 705 of the Communications Act of 1934.

Since Senator Leahy and I introduced the first version of this bill, S. 1667, the legislation has been substantially revised and improved. S. 2575 now enjoys the strong support of the Justice Department as well as major communications and computer industry groups and the American Civil Liberties Union.

Today, Senator Leahy and I will place before the subcommittee an amendment in the nature of a substitute for S. 2575 that makes several minor and technicalchanges in the bill. A summary of these has been distributed, and I will not explain each one. But I do want to call the subcommittee's attention to the last three changes listed on the summary sheet.

First, the Federal Communications Commission has brought to our attention the problem they have encountered in a recent highly publicized case of "jamming" of satellite cable programming. The FCC has suggested a new provision to clarify and strengthen legal protection against deliberate or malicious interference with satellite transmissions. Chairman Thurmond has suggested that this bill may be an appropriate vehicle for this important but non-controversial change, and we agree.

Second, a recurring concern throughout the consideration of this legislation has been the fear of liability for inadvertent overhearing of electronic communications. The changes made by the House have gone a long way toward allaying this fear, but to drive the point home, this amendment provides that only intentional acts of interception --- those meeting the highest standard of specific intent --- can be punished criminally.

Finally, the subcommittee has wrestled with another problem that was considered at length on the House side: criminal liability for unencrypted radio signals, particularly private satellite video transmissions.

The problem is to strike the right balance between privacy policy and the realities of physics. Individuals and businesses surely expect privacy when they participate in a private video-teleconference or, in the case of a television network, when they transmit raw news footage via satellite by a "backhaul feed." Certainly the law ought to enforce that expectation of privacy. At the same time, the engineers tell us that home satellite dishes may be able to receive some of this material, and that for truly private communications, encryption is a viable alternative.

The bill already contains substantial barriers to imposing liability on satellite dish owners: the exemption for cable programming and network feeds, for example, and the requirement of an "intentional" interception. But, at the urging of Senator Laxalt, Senator Grassley, and others, we have re-examined this issue. Our amendment wouldnot rule out a criminal sanction for intentional interception of private video transmissions via satellite; but it would reduce that sanction to the lowest possible level --- a $500 fine --- for the first offense. We believe this strikes the right balance: it defines these interceptions as wrongful, but takes into account the equities on the other side of the issue. But we also recognize that this resolution may not put the issue to rest. So we plan to continue to work with other Senators to fashion an appropriate solution for this narrow problem.

A SUMMARY OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968 -- the federal wiretap law -- to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law to update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunication technologies. Originally introduced in the Senate as S. 1667 by Senators Leahy and Mathias, and H.R. 3378 by Congressmen Kastenmeier and Moorhead, the bill has gone through a substantial revision as a result of negotiations with interested Senators and their staffs, various industry and privacy groups and the Department of Justice.

On June 11, the House Judiciary Committee unanimously reported H.R. 4952. On June 19, Senators Leahy and Mathias introduced that bill as S. 2575. On June 23, the House passed H.R. 4952. On August 12, the Subcommittee on Patents, Copyrights and Trademarks of the Senate Judiciary Committee reported S. 2575. During Subcommittee consideration some Senators expressed concern that the penalties for private viewing of certain satellite transmissions were too severe. Their concerns have been addressed by a reduction of the private and public penalties for home viewing. The bill also addresses the recent Captain Midnight incident by increasing penalties for interference with satellite transmissions.

The Justice Department strongly supports this bill.

Highlights of the Leahy-Mathias substitute to amend S. 2575, the Electronic Communications Privacy Act of 1986, follow.

- Currently, Title III covers only voice communications. The bill expands coverage to include video and data communications.

- Currently, Title III covers only common carrier communications. The bill eliminates that restriction since private carriers and common carriers perform so many of the same functions today that the distinction no longer serves to justify a different privacy standard.

- At the request of the Justice Department, the bill continues to distinguish between electronic communications (data and video) and wire or oral communications (voice) for purposes of some of the procedural restrictions currently contained in Title III. For example, court authorization for the interception of a wire or oral communication may only be issued to investigate certain crimes specified in Title III. An interception of an electronic communication pursuant to court order may be utilized during the investigation of any federal felony.

    - Wire communications in storage, like voice mail, remain wire communications.

- To underscore that the inadvertent reception of a protected communication is not a crime, the bill changes the state of mind requirement under Title III from "willful" to "intentional."

- Certain electronic communications are exempted from the coverage of the bill including

    - the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

    - tone-only paging devices;

- amateur radio operators and general mobile radio services;

- marine and aeronautical communications systems;

- police, fire, civil defense and other public safety radio communications systems;

- specified transmissions via audio subcarrier;

- the satellite transmission of network feeds;

- the satellite transmission of satellite cable programming as defined in Section 705 of the Communications Act of 1934;

- any other radio communication which is made through an electronic communications system that is configured so that such communication is "readily accessible to the general public," a defined term in the bill.

• The term readily accessible to the general public does not include communications made by cellular radio telephone systems; therefore, the bill continues current restrictions contained in Title III against the interception of telephone calls made on cellular telephone systems. However, the criminal penalty for an unlawful interception of a cellular phone call and similar communications is reduced from the current five-year felony.

  - under the Simon amendment that criminal penalty is reduced to a $500 fine.

• The bill expands the list of felonies for which a voice wiretap order may be issued. It also expands the list of Justice Department officials who may apply for a court order to place a wiretap.

• The bill creates a limited exception to the requirement that a wiretap order designate a specific telephone to be intercepted where the Justice Department makes a showing that the target of the wiretap is changing telephones to thwart interception of his or her communications.

- A telephone company may move to quash an order for such a "roving tap" if compliance would be unduly burdensome.

• The bill makes it a crime for a person who has knowledge of a court authorized wiretap to notify any person of the possible interception in order to obstruct, impede or prevent such interception.

• Title II of the bill creates parallel privacy protection for the unauthorized access to the computers of an electronic communications system, if information is obtained or altered. It does little good to prohibit the unauthorized interception of information while it is being transmitted, if similar protection is not afforded to the information while it is being stored for later forwarding.

• The bill establishes criminal penalties for any person who intentionally accesses without authorization a computer through which an electronic communication service is provided and obtains, alters or prevents authorized access to a stored electronic communication. The offense is punished as a felony if committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain; otherwise it is punished as a petty offense.

• Providers of electronic communication services to the public and providers of remote computing services to the public are prohibited from intentionally divulging the contents of communications contained in their systems except under circumstances specified in the bill.

- The contents of messages contained in electronic storage of electronic communications systems which have been in storage for 180 days or less may be obtained by a government entity from the provider of the system only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant.

- The content of messages stored more than 180 days and the contents of certain records stored by providers of remote computer processing services may be obtained from the provider of the service without notice to the subscriber if the government obtains a warrant under the Federal Rules of Criminal Procedure or with notice to the customer pursuant to an administrative subpoena, a grand jury subpoena, or a court order based on a showing that there is reason to believe that the contents of the communication are relevant to a legitimate law enforcement inquiry. Provisions for delay in notice are also included.

- An electronic communications or remote computing service provider may disclose to a non-governmental entity customer information like mailing lists, but not the contents of the communication. Disclosure of such information to the government is required, but only when the government obtains a court order, warrant, subpoena, or customer consent.

- At the FCC's request, a section was added to the bill to address problems highlighted by the recent Captain Midnight incident. The bill increases penalties for the intentional or malicious interference with satellite transmissions.

- The bill clarifies that telephone companies and other service providers are not civilly or criminally liable for good faith assistance to law enforcement agencies.

- Civil penalties are created for users of electronic communications services whose rights under the bill are violated.

- The Grassley amendment, which the sponsors have accepted, sets up a reduced penalty structure for the private home viewer whose reception of specified satellite transmissions is not for commercial gain.

The Simon amendment, which the sponsors have accepted, sets up the same penalty structure for the interception of radio communications transmitted under frequencies allocated under subpart D of part 74 of the FCC rules.

The penalty structure under the Grassley and Simon amendments is:

- A first offender will be subject to a suit by the federal government for injunctive relief. If injunctive relief is granted, the court may use whatever means in its authority, including civil and criminal contempt, to enforce that injunction. It must impose a $500 civil fine. In addition, the penalty for second and subsequent offenses is a $500 fine in a suit brought by the government.

- Under the private civil damages provisions of the bill, the first offender may be sued for the greater of actual damages or statutory damages of $50 to $500. The second offender is subject to suit for the greater of actual damages or statutory damages of $100 to $1000. Third and subsequent offenders are subject to full civil damages under the bill.

- The bill creates a statutory framework for the authorization and issuance of an order for a pen register or a trap and trace device based on a finding that such installation and use is relevant to an on-going criminal investigation.

SUPPORTERS OF H.R. 4952
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The organizations and individual corporations named below support the principles embodied in the legislation.

ORGANIZATIONS

- Electronic Mail Assoc.
- ADAPSO
- Telocator Network of America
- Cellular Telecommunications Industry Assoc.
- ACLU
- National Association of Manufacturers (NAM)
- U.S. Chamber of Commerce
- National Association of Broadcasters (NAB)
- National Cable Television Assoc. (NCTA)
- National Association of Business & Educational Radio (NABER)
- CBEMA
- U.S. Telephone Assoc.
- Videotext Industry Assoc.
- Information Industry Assoc.
- Electronic Funds Transfer Assoc.
- Radio and Television News Directors Assoc.
- Association of American Railroads
- Institute of Electrical and Electronics Engineers (IEEE)
- Direct Marketing Association
- Utilities Telecommunications Council
- Associated Credit Bureaus, Inc.

CORPORATIONS

- AT&T
- General Electric
- IBM
- GTE
- ITT
- MCI
- CBS
- ABC
- NBC
- Tandy Corp. (Radio Shack)
- Trintex
- Equifax
- TRW
- Source Telecomputing Corporation
- Chase Manhattan Bank
- Motorola
- Ameritech
- Bell Atlantic
- Bell South
- Southwestern Bell
- NYNEX
- Pacific Telesis
- US West
- Associated Credit Services, Inc.

June 10, 1986

SUMMARY OF CHANGES BETWEEN H.R. 3378 AND H.R. 4952:

The Subcommittee received hundreds of drafting suggestions during the four days of hearings, and in the numerous additional statements submitted for the record. Many of the suggestions (especially those from various telephone companies) were of a largely technical nature. These amendments were incorporated into the new bill where appropriate. The major policy- oriented differences between H.R. 3378 as introduced and the new bill, H.R. 4952, are as follows:

(1) Inadvertent overlap between H.R. 3378 and various computer crime bills has been removed. The Electronic Communications Privacy Act addresses problems relating to the transmission (and related storage) of electronic communications. Computer crime legislation is generally directed at unauthorized access to data in a computer. Section 102 of the bill as introduced is substantially modified so that it does not reach computer hacking.*

(2) New exemptions have been added to the types of interceptions which are not unlawful. These clarify the original intent that intercepting traditional radio services is not being included in the bill. The bill also clarifies that monitoring of shared channels is not unlawful. The bill also defines the key term "readily accessible to the general public". Thus, cellular telephones, private and public microwave services and voice or display pagers are protected against interception, but cordless phones and tone-only pagers are not.

---

* The amendment makes civilly and criminally liable a person who wilfully accesses an electronic communication system and obtains, alters or prevents use of the system while a communication is being stored as a part of the communication process. This variant on the interception crime is included because storage incidental to transmission is an integral part of the new electronic communication technology.

(3) The bill clarifies the rules under which the provider of an electronic communication service can disclose information to the government. The general rule is that if the government seeks access to the contents of a message during transmission they must seek a Title III type** warrant based on probable cause. If the government seeks access to copies of a message kept by the provider either before or after delivery (up to 6 months later) they must obtain a search warrant based on probable cause. If the government seeks to obtain access to the records of an electronic communication provider (or the contents of a message which has been kept for more than 6 months) they must obtain _either_ a search warrant, a court order based on "reasonable suspicion" which gives the user of the service an opportunity to contest access by the government, or a subpeona with notice to the customer.

Additional provisions are added relating to delayed notice, and cost reimbursement for system provider's cooperation with the government.

The service providers have thus agreed to be regulated and subject to suit by aggrieved parties in return for statutory protection for their records.

(4) The Department of Justice requested several additions and deletions to the bill. An explanation of changes incorporated in the bill is contained in a separate memorandum.

** Title III, 18 U.S.C. 2510 et. seq. imposes more procedural requirements than a search warrant, because the nature of the privacy interest being invaded is greater. Thus, only certain high level officials can apply for such a warrant, only for certain crimes. Title III also precludes a general search by requiring greater specificity and a more limited duration than a search warrant. Finally, because of the prevasive nature of the search the law enforcement officials must sift out non-incriminating conversations which are overheard.

On The Occasion of the Nation's First Telecommunications Privacy Week

Telecommunications Privacy and Our Freedom:

A lecture by Morton S. Bromfield

Wednesday, May 14, 1986 at 7:00 p.m.

Rabb Lecture Hall, Boston Public Library, Copley Square

Cosponsored by The American Privacy Foundation.

For more information please call 536-5400. extension 371.

The Public Is Cordially Invited.

May 12, 1986
ADVANCE COPY
PAGE ONE OF 12

TELECOMMUNICATIONS PRIVACY AND OUR FREEDOM

Co-Sponsored by The Boston Public Library and The American Privacy Foundation

[To Be Delivered by Morton Bromfield on May 14, Boston Public Library -- Rabb Hall 7:00 P.M.]

The Boston Public Library has hundreds of books on raising petunias, dozens on the culinary virtues of garlic, but only two devoted to wire tapping. Why?

The first of these two books — The Eavesdroppers by Sam Dash, later to be Chief Counsel of the Watergate Committee — was initially blocked from publication for a trumped-up reason. Finally a friendly Congressman threatened to hold televised Hearings, potentially giving much greater publicity to Dash's findings. Publication followed, in 1959. But why the roadblock then?

Today why do we all read of concern for computer privacy and see nothing in print on telephone privacy? After all, today's telephone system — the world's largest machine — is operated by a computer-controlled electronic switching system (ESS). We all recognize that once a computer is tied into the telephone system it becomes vulnerable to accessing or tapping by someone finding the access code. True, we all realize that computer hacks — kids — do this for fun, but isn't it just as true that adults can do it for profit and power? Yet we typically read what The New York Times put on its front page not long ago: "Computer Security Worries Military Experts: Most of the vulnerability...relates to computers tied into networks by telephone lines...The real threat may be posed not by the Soviet Union but by young American computer enthusiasts."

Simply put by computer security consultant Sanford Sherizen, if you can communicate out, someone else can communicate in. This rule of thumb applies to everyone's computer-switched telephone and to everyone's phone-linked computer. And it applies to adults for power and profit as well as to kids for play.

WHY TAP PHONES?

Computers store mostly historic records. But a wire tapped businessman or politician is explaining what he is doing, his plans, his reasons, his intentions. Tapping into a computer lacking such vital information is like robbing a graveyard.

So phone tapping by adult Professionals is fruitful. And, when used to fight organized crime through Court orders, beneficial. For nefarious purposes, however, wire tapping for such as industrial sabotage, with the ability to disrupt as well as eavesdrop, is the most cost-effective clandestine weapon. But above all wire tapping is a powerful tool for subversion. Our concern is political espionage and subversion by blackmail. The manipulation of our bureaucracy, as warned by this century's most read political scientist.

This is not to say that computer privacy should not be preserved. The looting and altering of medical and financial records can distress, even financially ruin a citizen. But may I emphasize that these consequences of lost computer privacy cannot destroy one's freedom. Wire tapping the conversations of our leaders in government, manipulating our centralized bureaucracy, can, however, lead to the domination of our every move.

EAVESDROPPING, AN ANCIENT PROFESSION

Getting back to the two books devoted to wire tapping. Why only two? After all, eavesdropping as a profession goes back to Saxon times, when a spy would stand outside a house, listening under the eaves. Put another way, a profession that existed before the Magna Carta, before Western democracies took codified form, came into being because of man's continuing, compelling need to know. According to an 1850's newspaper article, this pervasive need to know led to the climbing of the very first telegraph pole by a private sector wire tapper. Clearly wired communications and wire tappers have had a long-term affiliation.

In 1882, just six years after the invention of the telephone, the first patent was granted on an anti-wire tapping device. Six years after that a Kansas City undertaker invented a switch meant to prevent telephone operators from intruding on his business telephone and tipping off a competitor. Almon P. Strowger was finding that his wagon was often coming back empty when answering a telephoned request to pick up a body. Strowger's electro-mechanical switch in fact brought into being the automatic Central Office, still being used world-wide in many countries, in an updated form. General Telephone and Electronics — GTE — incidently, came into being by acquiring Strowger's patents.

Of course there are many more phones in use today — one for every citizen over age 15. And many more phone wires: wires that could stretch back and forth to the sun three times. And the same need to know. Why just two books?

A MICROWAVE MIRAGE

All 50 of our States' anti-wire tapping statutes require only proof of interception of wired messages. But for 34 years the federal statute intended to protect wired communications was crippled by also requiring proof of divulgence to a third party, oddly based on the earlier Radio Act's need to protect messages broadcasted into the air. During this period, in New York City, the "wire tapping capital of the world," there was one arrest under the Communications Act of 1934.

Divulgence as a required proof was dropped in the 1968 Federal statute. But today everyone is chasing the minuscule threat of microwave interception, leaving the great body of wired communications vulnerable still. We read almost daily of microwave interception. Microwave interception is a problem, but only part of the problem. Only some 5% of the 800 million daily domestic phone calls travel by microwave. But over 90% of today's phone calls travel through the 700 million miles of copper or fiber optic cables that are switched electronically by computer — a computer as vulnerable as any other computer linked to a phone line. Today computer privacy and telecommunications privacy are very much one and the same. And the wired communications network is the nervous system for both.

Why the outpouring of concern for the 5%? Why next to nothing on the literally and literarily buried cabling whose vulnerable terminals have been tapped undetectably at Central Office's ever since there were Central Offices. In 1968 an interviewed master wire tapper publicly revealed that all other forms of tapping were "old hat," that the "preferred method" is through a Central Office, in much the way that a legitimate answering service is connected.

To be sure the electro-mechanical Strowger switching put a stop to routine intrusion by a telephone operator. Adopted world-wide as a standard switch, plug-and-cord juggling by operators was made obsolete. When you rotary dialed with your forefinger, electric pulses at the Central Office mechanically connected you to your dialed party. But that is not to say that an operator or a private tapper couldn't tap on a non-routine basis. Proving the point in 1971, the Chairman of the last House subcommittee on Privacy read into The Congressional Record the woes of another undertaker. The Reuters dispatch described a French undertaker whose phone calls were being automatically switched — unbeknown to her — to a competitor. And, should you think that only undertakers have this problem, in 1973 when I first spoke to the head of all security for AT&T, Mr.

William Caming, he told me of a Manhattan locksmith whose business calls were being automatically forwarded — unbeknown to him — to a competitor.

So today, despite Almon P. Strowger's enterprise and thanks to the Bandaid security design of ESS, a phone tapper doesn't have to climb a pole, or burrow in a basement, or even pay off a telephone company employee. He can, for example, make illicit use of call forwarding. Or, he can open a quasi-legitimate answering service. Or with a computer keyboard linked into the phone system with a $300 modem, and with the current password or access code, a private tapper can remotely select and eavesdrop upon any subscriber's phone. The terminals of everyone's handset wires, known as the 'twisted pair', wind up on the main distribution frame at a Central Office. These terminals are the Achilles heel of today's telephone system, vulnerable not only to technically undetectable wire tapping, but also to induced "technical difficulties": false busy signals, false ringing not heard by the party you dialed, distorted voices, faint voices, echos, static, disconnects, consistent misdialed numbers, slow dial tones and et cetera.

Summing it up in four words, on June 7 of 1983 I interviewed an ex-wiretapper, presently technical director of one of the largest computer/electronics magazines. "Wire tapping," he said, is "easy as hell."

A BANDAID APPROACH TO TELECOMMUNICATIONS PRIVACY

The lack of safeguards in today's computer-controlled switching system is just the latest manifestation of the phone company's traditional laxity. How did this critical lapse come to be? How could Bell Labs, creators of the transistor, create privacy-blind ESS exchanges? If computers can be designed to do "anything," why did the computerization of our telephone switching system make eavesdropping easier than it had ever been before?

The development of the ESS exchange was the largest project in the history of Bell Labs. If privacy was a design goal, it certainly couldn't have been a major priority. Serious work began in the 1950's, with field trials targeted for 1959. However, the budget of $45 million exploded into an expenditure of some half a billion dollars, and the first ESS office didn't get into operation until 1965.

The project was branded "the Lab's greatest single mistake." The first system, located in Elizabeth, New Jersey, was rendered almost totally inoperative by radio transmissions from aircraft over nearby Newark Airport. The ESS exchange, evidently, was demonstrably vulnerable to radio intrusions. This embarrassing oversight was quickly rectified, but in a piecemeal manner. This haphazard approach to system integrity was never replaced by a more cohesive one. The first ESS exchange, recognized to be vulnerable to even accidental intrusion, was reproduced in major population centers across the nation at a cost of twenty million dollars per installation, without developed safeguards.

Included in the signaling technology between a subscriber and an ESS exchange is the so-called "E-signal, musical note 'E'." The signal is the tone generated by a touch-tone telephone, actually 2637 Hz. It tells the electronic switchgear the number that the subscriber is dialing. But other sounds at frequencies close to this one or even background noises can be mistaken by the hardware for a legitimate signal:

> "A woman in the midwest complained to her local phone company that her calls were frequently disconnected in the middle of a conversation. Servicemen went out to the premises. Nothing. Bell Labs was consulted. It was found that the woman possessed a highly peculiar laugh that would put out a sound similar to the signaling equipment. The network equipment, when it heard this tone [2600 Hz.], thought she had hung up."

But radio from jets and peculiar laughs were not the only unforeseen access problems overlooked by the developers of ESS exchanges. Washington's ESS exchanges had another variation:

> "...there was a coin phone in Washington, D.C. Every time a car crossed the trip wire at a nearby gas station, conversation would be disconnected. The Labs had to do some trickly design work on [the signaling tones]."

Altogether ESS was developed with either no thought or with some thought given to those that make a business of eavesdropping electronically.

AN INVISIBLE INDUSTRY

Last October Congress' Office of Technology Assessment (OTA) completed a one and a half year study, "Electronic Surveillance and Civil Liberties." As its first and foremost conclusion, as an intended warning, it stated:

> "The extent of use of electronic surveillance in the private sector is uknown."

This study included the efforts of twenty advisory board members from academe and industry. It was a prolonged, well-funded, serious attempt to investigate what Senator Sam Ervin bravely declared in 1970 — before Watergate — had been "underground for decades." Now it became official: A silence barrier, even to this day, surrounds the wire tapping industry.

Didn't Watergate bring illicit wire tapping to the surface?

Interestingly enough, it was Sam Dash's book The Eavesdroppers that brought him to the attention of Senator Ervin. As Chief Counsel of the Watergate Committee, Sam Dash was well-placed to deal with wire tapping. True, the bugging of the Democratic National Headquarters was addressed. But no instance of wire tapping came into his attention. And this was not accidental.

Evidence and testimony of wire tapping — not bugging — was submitted by The American Privacy Foundation, by me and APF co-founder Charles Witter, the former Chief Aide of the Congress' last House Subcommittee on Privacy. To whit: once Senator McGovern was nominated, after the publicized break-in at the Watergate, his H Street headquarter's phones were tapped, both for eavesdropping and disruption, right up to the November elections. Mr. Witter later determined that the staff aide referred to us was not Scott "Parr," as we were told, but Scott Armstrong. (Later he would write a book on the Supreme Court, The Brethren.) Armstrong falsely assured us that Sam Dash had our information. Sam Dash was never told and he never got our testimony.

In fact there has never been a successful government investigation of illicit wire tapping. The National Wiretap Commission began operation in 1972 to measure and ensure the operating effectiveness of The Omnibus Crime and Safe Streets Act of 1968. This was the most ambitious effort ever intended to investigate illicit wire tapping. It was well staffed, fully funded and had subpeona powers. American Privacy Foundation co-founder Professor Vern Countryman wrote a detailed letter to its Director, focussing on tapping at Central Offices, the "preferred method" of the Pros. He got in return two "non-responsive replies." A scheduled Hearing was inexplicably cancelled. True, the Minority Report did complain in general that illicit wire tapping was not investigated. But, more to the point, though Commission member Professor Alan Westin "vehemently promised" coverage of Central Office wire tapping in the Minority Report, nothing was put into print. And, as detailed in Chapter Six of our book, this investigation failed in a way that revealed no failure.

LINKED HIGH COURT IMPROPRIETIES

Not only the Congress has problems in looking into and redressing wire tapping abuses. Our highest Courts become immobilized when addressing matters of interest to the wire tapping "lobby."

While researching for our book at the Federal Communications Commission, I got a tip that the 600 page Plan for the divestiture of AT&T had not one word on telecommunications privacy. Fortunately Federal District Court Judge Harold Greene had demanded that Tunney Act statute procedures be used by Justice and AT&T so as to ensure that the public interest would be served. The ACLU agreed to file in Judge Greene's Court Tunney Act Invited Comments similar to ours. We asked merely that the 39 words of AT&T's Open Door Policy, with AT&T "since its inception," be incorporated in the charters of the seven Bell Operating Companies. This would assure access to Central Offices for investigating illicit wire taps. Greene, however, consciously violating both Tunney Act and Federal District Court procedures, ordered APF and ACLU Comments not to be docketed — that is, they never officially existed. And he verbally chastized the head of Justice's Task Force, James Denvir, for formally referring our Invited Comments.

To redress Judge Greene's improprieties, this Foundation submitted a Motion to the U.S. Supreme Court. The highly concerned Chief Clerk, Alex Stevas, came in early to read it, write a forwarding Memorandum, and distribute the Motion to the nine Justices. It was deliberated upon by the Justices and rejected in a letter to Stevas. But it never appeared on the Notice List, as all reviews must. Officially it never existed.

These last-minute efforts to preserve the legal toehold on telecommunications privacy thus failed. And when the divestiture plan went into effect, access into a Central Exchange to investigate wire tapping by the Pros was lost to us as citizens. No access, no proof; no proof, no case. I asked a senior FCC official at the time what he would do to investigate wire tapping complaints once the Plan went into effect. Said attorney Lou Feldner: "You have raised a very serious question."

This Plan, this disarming of our Federal wire tapping statutes, this Privacy Lobotomy, went into effect on the first day of 1984.

A "CAPTIVE" AGENCY

As you may know, the FCC came into being along with the Communications Act of 1934. Its "paramount and continuing responsibility" from the outset was "to ensure the integrity of the communications network." And at the beginning this regulatory agency did its duty. Early on its "raiding squad" discovered taps on the phones of the Supreme Court Justices, put there by private sector wire tappers. But several interesting consequences: First, as Sam Dash wrote, "apparently the Justices were never informed." Then, news of the raiding squad's discovery didn't come to light for fourteen years — in testimony by the former head of FCC's Telephone Division. Last but not least, the raiding squad was never heard from again.

And in 1982 when I interviewed the FCC attorney who said he knew more about wire tapping than any other attorney in the agency, I asked him how many wire taps he had discovered in his more than ten years in the Enforcement Division. Said Roger D. Hertz: "Never had a wire tap proven."

Last July 3, on the strength of offering to testify in a letter to FCC Chairman Mark Fowler, I met with staff members and broke longstanding "ice." (In 1964 The Naked Society told of the FCC's "incredible evasiveness" regarding wire tapping.) The staff freely admitted to a "mistake" in transferring the all-powerful authority to investigate wire tapping complaints to Justice. Moreover, they urged me to get a parallel investigation going in the Congress.

On July 18 came a Memorandum to me from the Office of FCC Chairman Mark Fowler "...will be more than happy to accommodate you with your letter request for an oral presentation." But on July 30, a knowingly false and misleading letter to this Foundation from their Director of Congressional Affairs denied jurisdiction "over wire tapping matters." Thus the recommended En Banc Meeting, a presentation to the five Commissioners, that would be covered by The New York Times, Newsweek and the MacNeil/Lehrer Report, has been estopped.

But let us return to this denial of jurisdiction over wire tapping. Are you shocked by this? Probably not. But let us suppose that the Federal Aviation Administration announced that it, without authority from the Congress, and without mandatory notification in The Federal Register, was transferring its responsibility for aircraft safety to the Criminal Division of the Justice Department. That would create widespread concern. People would at least want to know why. And people would want to know that the Criminal Division would do what the FAA had been doing. May I suggest that the FCC's silent shift of responsibility does not shock you because all aspects of the wire tapping industry and its "lobbying" — if you will — its lobbying in Washington are covert operations.

And now that you know, ask your congressman to find out why the Criminal Division — doing a fine job chasing down computer hacks — is doing very little about chasing down professional wire tappers.

John Kenneth Galbraith has a ready explanation for failed efforts of regulatory agencies: "Very often," he wrote, an agency becomes "the captive" of the industry it is intended to regulate. One could jump to the conclusion that in this case the telephone company — formerly AT&T and now the Bell Operating Companies — became the captor of the FCC. But note, for instance, that the Anti-trust Division of the Justice Department had no problem breaking up the largest company-employer in the world. Yet when it came to matters of interest to the wire tapping industry, not only Justice but the FCC, and the Federal District Court, and the U.S. Supreme Court, all were stopped dead in the water in attempts to move toward telecommunications privacy. And these defeated efforts, all of them, left a string of lawless acts, acts that were never recorded or reported.

"AN EMERGING POLICE STATE"

Perhaps the author of the second book devoted to wire tapping, published in 1968, can offer us insight. Bernard Spindel was the acknowledged dean of wire tappers. For example, I was told by an ex-wire tapper that Spindel had so profusely bugged the Manhattan headquarters of Revlon, the international cosmetics firm, that, if the building's steel structure failed and fell, the building itself would have been supported in place by his wiring. But Spindel, more than anyone on record, realized the potential for subversion, blackmail, manipulation. In The Ominous Ear, he wrote:

> *"This book is a factual account of a surreptitious art that possesses more power than the largest H-bomb devised by man. Nations have been born and governments overthrown..."*

Added Justice William O. Douglas: "Power tends to form a government of its own."

But closest of all is the observation of former Congressman Cornelius Gallagher. He headed a House Subcommittee on Privacy for seven years. A committee, incidently, that for no given reason was debarred from investigating wire tapping. In 1971 Tip O'Neill arranged a meeting. Gallagher judged that what I saw as the manipulation of the telephone company by the wire tapping industry and what he saw "as the emerging police state are two facets of the same threat."

But that was fifteen years ago. If a police state is "emerging," why can't we see more evidence of it today?

When Rachel Carson warned the world twenty years ago through her book Silent Spring, it generated world-wide concern for the ecology. Even the title made the point beyond doubt. But in a sense, Silent Spring need never have been written. For as pesticide technology advanced, soon enough sullen skies, barren land, poisoned water, and deformed life would have made Carson's point unmistakably.

But swiftly advancing surveillance technology is having the opposite effect. The better it gets, the less visible it is. The more destructive it is to freedom, the less privacy seems to be disturbed.

Is it possible that the perfection of surveillance techniques and clandestine expertise has obscured signs and deeds fulfilling Orwell's warning? Could we be drifting toward a covert police state?

LESS THAN FULL DISCLOSURE

One book that did get published on this generalized subject was The Age of Surveillance, in 1980. It was written by a civil liberties attorney and former Director of the ACLU's Project on Political Surveillence, Frank Donner. One would suppose that a book with this title and over 500 pages –the thickness of a phone book — would reveal all. Its dust jacket indeed has appropriate laudable comments from such civil libertarians as Nat Hentoff and Father Robert Drinan: "...a monumental and eloquent history and theory of the ways in which the state has kept track of us..."

But this book overlooks the fact, for example, that there are two forms of surveillance, the usual cold surveillance — when someone follows you surreptitiously — and "hot" or "rough" surveillance, when you are met at every turn by tailers each of whom blatantly use repeated motions or sound signals to unnerve you. This book also neglects to mention that there are two kinds of "bugs." The one we all know which is a micro-miniaturized transmitter that picks up a target's conversation, even his breathing, if hidden in his clothing. But there is no mention of radio bugs. These are micro-miniaturized receivers that, all but invisible and without wires, can be planted in seconds in your car, your office, your home. Used in conjunction with transmitter bugs, a targeted citizen can be plagued with strange sounds, when no one else is with him.

In reading over a hundred books I did find one, not naming, but describing an in-place radio bug. The target was being harassed, he believed, by the subject of his lawsuit — AT&T. Jim Ashley figured out that the music he was hearing in his car couldn't be coming from his radio, which was shut off. But his quote in the well-written book, The Biggest Company on Earth, was completely discredited by an extraneous sentence planted within the quote.

What do you suppose was included in The Age of Surveillance's 500 pages on the subject of phone tapping? Well there are two fleeting, tangential mentions, explaining to the reader that a court order is required in order to wire tap.

May I leave with you a state-of-the-surveillance-art statement to be remembered when you leave this place of learning dedicated to free citizens, one that I daresay you will read nowhere else:

> Any room of any house, in any building serviced by a conventional phone line can be quickly turned into an observation/listening chamber. Conventional phone lines can be used to provide power to state-of-the-art micro-miniaturized bugs and video cameras. And these same "twisted pair" with today's operating technology, can be used to carry the eavesdropped audio and video signals to any other location serviced by a telephone line — a hotel room in Cannes, France, if you like. And by dialing from the remote listening post, the features of the so-called Infinity Transmitter can be used to avoid detection. Is someone about to electronically sweep the office you bugged? Simply dial all but the last number of your target's phone number, and you can deactivate your hidden transmitter — no signal, no detection.

COST-EFFECTIVE SAFEGUARDS FROM AVAILABLE TECHNOLOGY

Are there countermeasures available to defeat this abuse of our phone network? Two years ago Pennsylvania Bell adapted one of its Central Offices to Western Electric's Convenience Package. This is a smart phone — the computer chip is in the handset — that, for example, will record, store, and play back to a subscriber the phone numbers that rang his number while he was away from his home or office. Not this exact technology but this kind of technology fitted to a Central Office can protect subscribers by storing what is called an "audit trail." Prolonged unauthorized connections to a subscriber's lines would be recorded on an uneraseable punched paper tape. And, just as no-notice audits are made of member banks of the federal banking system, irregular inspections of the CO's equipment would ensure intended protection.

This was explained to Congressman Barney Frank and he asked, "How much?" We estimate some $350 million to develop the technology, the hardware, the software, and fit out the 800 or so ESS Central Offices presently handling over 90% of all phone calls. No small amount, to be sure, but AT&T's last reported profit before divestiture was some six billion dollars.

We come back to last October's intended warning by Congress' Office of Technology Assessment: "The extent of use of electronic surveillance in the private sector is unknown." It is all well and good for the government, attempting to protect us, to officially state that they don't know what the wire tapping industry is doing. But on a personal level, we average citizens face a dilemma, in fact an embarrassment leading to more silence on the subject.

ILLICIT WIRE TAPPING "DOESN'T EXIST"

In December of 1983, in the course of researching for our book, I visited the Security Division of the Chesapeake and Potomac Telephone Company. I am now disguising the names of the two C & P attorneys, for reason that will be made clear. I ask: "...What do you do when a customer complains about a suspected illicit wire tap?"

Mr. "Henry" answers that 90% of the time it is cleared up on the telephone with a telephoned explanation from the Repair Department. He adds that in the telephone company's other 10%, a visit is made by the Repair people and it is found to be only a malfunction of equipment.

"Well, 90 plus 10 equals 100. Have there never been any illicit wiretaps found in your eight years?"

"No, never since I've been with the company."

I turn to Mr. "Short": "How long have you been with the Security Division's Legal Department?"

"Eleven years — and never during my time here have any illicit wiretaps been found."

"Are you saying that there is no such thing as an illicit wiretap?"

Short, with emphasis and finality answers, "They don't exist!"

"Excuse me, please, I would like to write this down."

"I didn't say that. Don't you say I said that. "Henry" is a witness. I didn't say that. And if you say I said that I will take you to court. What I said was, I had no knowledge of any."

This lawyer-like defense is highly effective. You are stopped in your tracks. Your phone company representative or the Criminal Division of the FBI could and do ask: "What proof do you have?" If the tapping is being done professionally, and you can't get access to a C.O., just leave.

As a further embarrassment, you may be asked, "Who is doing it?" Obviously, if the Congress can't find anything out, you cannot say. But let us look further.

GRADUATING FROM THE FEDERAL CAMPUS

Libyan dictator and godfather of international terrorism Colonel Muammar el-Quaddafi is much in the news lately. Piecemeal he is using with great effect twenty-one tons of extremely powerful plastic explosive supplied by an ex-CIA agent. Edwin P. Wilson left the CIA to amass $15 million, using the Old Boys Network and cover of purported CIA operations to aid his entrepreneurial efforts. Mr. Wilson also used many of the clandestine techniques learned at taxpayers' expense while on the Federal Campus. But for the zeal and diligence for three years by a young U.S. attorney, Wilson would have gotten away clean. The CIA and the FBI treated its "graduate" rather kindly, given what they knew of his operations.

But there are many more graduates from the Federal Campus. A decade-old figure puts the number at more than 200,000. One of the many books exposing FBI operations [try to find one exposing industrial espionage] quoted a Congressman: "There sure are a lot of them around."

The author of Spooks, The Haunting of America, The Private Use of Secret Agents, described the formation of Intertel, an international private detective agency, as "skimming the cream" from federal intelligence agencies. Added Barron's magazine reporter and author of a book detailing Intertel's heavy operations, Ms. Gigi Mahon:

> "Intertel is quick to point out that it never hired anyone out of public service until they first "retired." But these people were not sixty-five years old; most were in the prime of their careers."

The wire tapping industry is staffed with many such graduates. At the very top of the surveillance elite's hierachy, they not only can rely on the Old Boys Network, but in the course of working for members and agencies of our government create ties, if not bonds. As a minor example, wire tapping is taught at The Federal Law Enforcement Institute at Glenco, Brunswick, Georgia. The expert teaching the subject is from "a large private firm" — the interviewee would not name it. But he did admit that tapping through a Central Office was mentioned there.

Of a more serious nature, Intertel worked in behalf of President Nixon to suppress evidence of an alleged deal between Nixon and ITT — a $600,000 campaign contribution in exchange for favorable anti-trust actions against ITT. You may remember the Dita Beard Memorandum published at the time by Jack Anderson. Thanks to the combined efforts of Intertel, the in-house spooks of ITT — also graduates from the Federal Campus — and a CIA-front company with offices across from the White House, Dita Beard was discredited and made to recant, and the longest Senate confirmation hearings ever — the Kleindienst Hearings — became "muddled." And they became muddled despite the efforts of such respected Senators as Phil Hart, Birch Bayh, Ted Kennedy and John V. Tunney. Altered documents and the three D's of the wire tapping pros — deceit, deniability and dirty tricks — took their toll. There was no defense for these insidious tactics then. There is no worked-out defense by any congressional committee now.

But it is an ill wind that blows no good. First, we have an eloquent example, now documented in our book, of how clandestine expertise can nullify what President Wilson considered the single-most important function of the Congress — to investigate wrongdoing. Second, realizing that the Hearings were made meaningless, John Tunney created legislation requiring all proposed anti-trust settlements — usually out-of-court — to be put before the public for Invited Comments and Federal Court review. It is on this thread — the violations of Tunney Act procedures — that hangs the one way in which telecommunications privacy can be achieved.

POLITICAL PARALYSIS

You might ask: "Can't our lawmakers enact new legislation?" Theoretically, yes. But it was in 1964 that a nationally syndicated column headlined: "Sword of Damocles Over Washington: lawmakers are seduously avoiding telephones." And it was that same year that Vance Packard's The Naked Society characterized the FCC's handling of its wire tapping responsibility as "incredible evasiveness." Added Jack Anderson, just before Watergate, "The apprehension over hidden bugs and taps has become so acute in Washington that officials at the highest levels guard their utterances as if the walls had ears."

More to the point, David Kahn, author of The Codebreakers recently put it this way: "A Senator's aide, with tongue half in cheek, said 'Let me put a tap on a Senator's phone for three weeks and I will own him'."

Whatever the reason, almost without exception, no congressman today will take meaningful action against illicit wire tapping.

Existing Federal wire tapping legislation is in fact adequate. What you read about is Congressional activity augmenting these to include, for example, protection of the communication of data as well as voice signals. But do not confuse motion with progress. Our telephone network of 700 million miles of cables was not being protected by the enforcement of adequate legislation even when the law could reach into Central Offices. Now a Microwave Mirage distracts our attention from where the real problem lies buried.

A half century ago The Communications Act of 1934 was hobbled by "confusion" with microwaves. History is repeating itself, all to the benefit of an underground industry: Today, if you please, we are told that one of the major advantages of the new fibre optic trans-Atlantic cable in the works is that it will provide phone security unavailable with present overseas calls sent via satellite by microwave. The vulnerable terminals of the new fibre optic cable will be at the Central Office — available for tapping by kids or adults, as usual.

The scene in Washington today can best be characterized by the aftermath of OTA's attempt to report on the wire tapping industry. A month after the study was published, I handed to Assistant Director Dr. John Andelin the very information he sought. He immediately concluded "Very valuable." Earlier, Bob Kastenmeier, the Congressman who initiated the OTA Study, given a rough idea of this Foundation's research from Congressman Barney Frank, became interested and I was asked to meet with a committee during the last Christmas recess. But now the attorney won't meet and Mr. Kastenmeier has lost interest.

Moreover, the Chairman of the one House committee that has oversight of the FCC will not merely assure the courageous Chairman of the FCC, Mark Fowler, that he indeed has jurisdiction over wire tapping mattjers. And Tip O'Neill, handed citations from FCC documents establishing beyond doubt their jurisdiction, tells me: "I can't help."

So now we have a Silent Speaker to match a silenced Federal District Court Judge, and, of course, a silence barrier still surrounds private sector wire tapping.

ORTHODOXY AND UNCONSCIOUSNESS

The average citizen will never be wire tapped and therefore will never know the gut-renching fear. He will surely wonder how uncontrolled wire tapping could lead to a police state. And yet this is the warning of such men as Orwell, Douglas, and B.F. Skinner. Power does tend to form a government of its own, and unlimited, instantaneous, technically undetectable wire tapping is power personified. In keeping with the palpable fear of wire tapping in Washington, almost without exception, those that have helped me over the years have done so furtively.

The Constitution intended ultimate political power to be in the hands of the governed. But information regarding the vulnerability and abuse of our telecommunications network is being withheld and manipulated. Our free society will not long withstand such a meaningful loss of privacy.

We have reached a stage predicted by Orwell — the stage of "...not thinking — not needing to think." "Orthodoxy," he said, "is unconsciousness." The pervasive silence, for decades, surrounding the activities of the wire tapping industry assures no thinking — unconsciousness.

And if one is technically minded and therefore concerned, he is told that the privacy of telephone-linked computers is impossible to achieve (statement by an FCC official). Or, as we have seen, one is told that "[illicit] wire tapping doesn't exist." We are led to doublethink: To believe that secure telecommunications are impossible and that the government is the guardian of telecommunications privacy.

Today's lapse seems narrow. But as we neglect the link between privacy and freedom and concern ourselves instead with telephone rates, we go where Orwell, with deep misgivings, leads:

> *"And when they became discontented, as they sometimes did, their discontent led nowhere, because without general ideas, they could only focus it on petty specific grievances. The larger evils invariably escaped their notice."*

Why should there be a long-standing silence barrier surrounding the wire tapping industry? Why should our Congress be frozen in fear? Why should every American think he is being protected, while in a conspicuous police state every Russian realizes he can be wire tapped at any time? Could this country, where liberty has been so carefully guarded for so long have caused the development and use of more sophisticated clandestine tools and techniques for destroying privacy and freedom? Have we been duped by the sophisticated use of disinformation? Could we be drifting toward a covert police state?

Sixteen years of research comes to simply this: Enforce all privacy laws to the hilt save one — on wire tapping — and a covert police state can be.

Shortly before the FCC silently transferred its all-powerful authority to investigate illicit wire tapping complaints to the Justice Department into the hands of those of the surveillance elite still on the Federal Campus, these poignant, prescient words were written by a political scientist:

> *Until they become conscious they will never rebel, and until after they have rebelled, they cannot become conscious.*

And we ask: *Why only two books?*

END

[IMPORTANT: ASK AUDIENCE PERMISSION TO TAPE Q & A PERIOD.]

THE AMERICAN PRIVACY FOUNDATION
13 EATON COURT, WELLESLEY HILLS, MASSACHUSETTS 02181

STATEMENT OF TANDY CORPORATION

On S.1667, The Electronic Communications
Privacy Act of 1985

December 13, 1985

Tandy Corporation ("Tandy") herewith submits its statement regarding S.1667, a bill to amend the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Act") relating to interception of private communications through "wiretapping" and "eavesdropping". 18 U.S.C. §2510 et. seq. S.1667 would extend the protection accorded such communications to encompass, with specified exceptions, messages, either analog (i.e., voice) or digital (i.e., voice or data), transmitted via a "wire, radio, electromagnetic, or photoelectric system that effects interstate or foreign commerce."

I. Introduction and Summary

Among its business interests, Tandy is a manufacturer and distributor of both telephone and radio transmitting and receiving equipment -- e.g., cellular and cordless hand-sets, short-wave radios, citizen band radios ("CBs") and police and public safety band-scanners. Indeed, through its 4,400 "Radio Shack", 450 "Radio Shack Computer Center" and 130 "Radio Shack Telephone Store" sales outlets, Tandy serves over 29 million American families, and is the largest retail distributor of consumer electronic products in the United States -- a position that it has acquired through its more than 65 years of service to the public. As S.1667 would impact either directly or indirectly virtually all of the communications services in which electronic equipment is designed to operate, Tandy would like to take this opportunity to provide the Subcommittee with its perspective on the pending legislation, a perspective that through Tandy's position as the number one retailer in the industry is necessarily attuned to the ever-changing needs and desires of the consuming public.

Tandy agrees with Senators Mathias and Leahy and their House colleagues, Representatives Kastenmeier and Moorhead, that the extraordinary developments in the telecommunications industry since 1968 have made obsolete the provisions in the Omnibus Act relating to privacy in communications.[1] The advent of new voice and data transmission facilities and services -- for example, "electronic mail", telecopying services and cellular telephony -- have, in fact, dramatically altered the personal and business communications environment. But, to date, there has been no accompanying evolution in the law to provide privacy protection for categories of communications that were not contemplated at the time of enactment of the Omnibus Act. Nevertheless, in order to foster the development of emerging communications industries, such protection may be necessary to ensure that individuals and businesses alike may protect not only their personal privacy, but their economic interests as well. S.1667 is designed to extend protection to new categories of communications, and the Subcommittee is to be commended for addressing this vital question.

Tandy supports the extension of privacy protection via S.1667 to analog cellular communications as well as to all forms of digital communications. Given the technology of the cellular industry, including the hand-off of calls from cell to cell, the cellular telephone subscriber simply does not differentiate between cellular calls and conventional landline telephone calls. The subscriber thus perceives that, like wire communications, celluar calls are private and protected from interception. Digital transmissions -- i.e., the transmission of voice or data through a series of signals representing digits -- are, for all intents and purposes, encoded, and thus also appropriately the subject of an expectation of privacy, whether transmitted by wire or radio. Accordingly, extension of Omnibus Act coverage to cellular and digital communications will not only encourage the development of those industries, but will, in fact, conform existing statutes to the public's perception of those laws.

---

[1] See Opening Statement of Senator Charles McC. Mathias, Jr.; Opening Statement of Senator Patrick Leahy; Statement of the Honorable Robert W. Kastenmeier; Statement of the Honorable Carlos J. Moorhead.

Tandy's sole, and limited, concern with S.1667, as drafted, is that the bill may be over-inclusive and extend privacy protection to categories of communications in which there has never been any perception or expectation of privacy. For example, as proposed S.1667 would proscribe the "willful" interception of ship-to-shore communications. As an alternative, Tandy proposes that an approach, similar to that recently pursued by the California legislature (California Senate Bill No. SB 1413), should be considered, and S.1667 revised to proscribe the willful interception of digital transmissions or of analog communications transmitted between cellular radio telephones or between a cellular telephone and a landline telephone. This more narrow framing of the legislation would enable Congress to extend privacy protection to the evolving communications industries without unduly imparing the public's right to use its existing investment in radio receiving equipment.

II. The Proposed Legislation

S.1667 proposes to extend privacy protection to all electronic communications -- including both analog and digital transmissions -- with certain specified exemptions. These exemptions are, essentially, four in number: (1) communications designed to be "readily accessible to the public"; (2) communications transmitted for the use of the general public relating to ships, aircraft, vehicles or persons in distress; (3) communications transmitted by a walkie-talkie or a police or fire communications system designed to be readily accessible to the public; (4) communications transmitted by an amateur radio station operator or by a CB radio operator. S.1667, Section 101(b). While the bill thus permits the use of walkie-talkies, CBs and police or public safety band-scanners (provided that such scanners monitor solely bands "readily accessible to the public"), it extends protection to other categories of transmissions broadcast over the public airwaves, including cellular telephone and ship-to-shore communications.

Tandy endorses the extension of Omnibus Act coverage to all cellular communications. Indeed, it is clear that the typical cellular subscriber perceives and expects privacy in his or her cellular conversations. The Congressional Office of Technology Assessment has thus concluded:

> The public generally expects that telephone conversations are private and that electronic surveillance of telephone calls is illegal, except in very narrowly circumscribed law-enforcement and national security investigations. . . . [T]he new telephone technology was not envisioned when current legal protections were enacted, and thus the statutory protection against telephone surveillance is weak, ambiguous, or non-existent.[2J]

In short, the similarities between landline and cellular service both in appearance -- e.g., the physical configuration of the subscriber handsets -- and service -- e.g., low call blocking rates and high grade of service -- have engendered in cellular subscribers the belief that their communications are "private." Indeed, giving the technological underpinnings of a cellular system -- e.g., the hand-off of calls and frequencies from cell to cell within the system's service area -- such a

---

[2J] Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington, D.C.: U.S. Congress, Office of Technology Assessment, OTA-CIT-239, October, 1985) at 29.

perception and expectation of privacy is neither unjustified nor unwarranted.

As a policy matter, Tandy believes that extension of privacy protection will help ensure the continued growth and vitality of the cellular industry. From a functional standpoint, should protection be denied the industry, cellular service would become less attractive vis-a-vis landline service. As the cellular industry is now in its infancy, denial of privacy coverage could well significantly impair the competitive viability of cellular technology. Tandy thus submits that the extension of privacy coverage to cellular communications could well serve the dual goals of fostering competition among the communications services, and encouraging the utilization of state-of-the-art technology.

Tandy also endorses S.1667's extension of privacy protection to all digital transmissions. As noted, these communications are transmitted in a "coded" -- in this case, digitized -- format. Accordingly, through the act of digitizing, the message sender has evinced an expectation that these communications should be "private". Thus, like the cellular subscriber, the message sender apparently perceives that existing law protects his or her communications. But, as digital services have developed principally since enactment of the Omnibus Act, to date, privacy coverage is not afforded these messages. Tandy supports the Subcommittee's proposal to update the Act to encompass these evolving technologies and to conform existing laws to the public's perception of the scope of privacy coverage..

III. The California Approach

Tandy endorses the extension of Omnibus Act coverage to all cellular communications, but believes the bill should be amended to make it clear that it remains permissible to use scanners to monitor walkie-talkie, CB, police or public safety or ship-to-shore communications -- in other words, those communications that are now and historically have been "readily accessible to the public."

Tandy is, therefore, concerned that S.1667, as drafted, is overly-inclusive. Although the bill is aimed primarily at affording cellular communications and data transmission services privacy protection, it nonetheless prohibits the willful interception of all electronic communications, save for the specified exemptions. While amateur radio, CB and police and public safety band communications are excluded from protection, S.1667 extends coverage, for example, to ship-to-shore communications. Unlike cellular communications, however, these messages traditionally have not been thought by the message senders to be subject to privacy protection. The United States Court of Appeals for the Ninth Circuit has acknowledged, for example, that "scores of mariners. . . listen to the ship-to-shore frequency."[3] Given this fact and given the many years over which the maritime public has become used to monitoring ship-to-shore frequencies, extension of privacy protection to these communications is not warranted. Indeed, a monitoring of maritime frequencies obviously has significant public interest benefits, as S.1667 itself recognizes by excepting from protection communications intercepted relating to ships, aircraft, vehicles or persons in distress. While the intent underlying this exception is commendable, Tandy believes that the overall prohibition on monitoring ship-to-shore frequencies will greatly diminish the likelihood of a distress call being intercepted.

Tandy believes that the perhaps inadvertent impact of S.1667 on communications services to which there is no perception or expectation of privacy would be great. While the exact numbers are not available at this time, Tandy estimates conservatively that there are over 350,000 amateur radio operators in the United States, each typically owning more than one receiver; that there are between 40 to 60 million CBs and walkie talkies operational within the country; and that there are over 50 million short-wave multiband receivers. In total, there are perhaps over 120 million receivers which potentially could be affected by S.1667. Clearly, legislation with the potential for such enormous impact upon the populace, and its accumulated investment, warrants careful consideration.

---

[3] United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (emphasis added).

In order to assure that equipment owners are not prohibited from maximizing the utility of their investment, Tandy proposes that the Subcommittee consider an approach paralleling, in part, that recently pursued by the California legislature in its deliberations on California SB 1413. Therein, the State legislature proposed to impose criminal penalties upon persons intercepting communications involving cellular radio telephones on either, or both, ends of the communication. A parallel approach here would result in a more narrow framing of S.1667. Specifically, Tandy suggests that the Subcommittee consider legislation extending Omnibus Act coverage to all digital transmissions and all communications transmitted between cellular radio telephones or between a cellular radio telephone and a landline telephone. In this manner, protection would be afforded to, and the further development encouraged of, the new technologies which have evolved since adoption of the Omnibus Act. At the same time, however, the legislation would be framed in the narrowest manner possible to satisfy this goal, and the inadvertent impact upon other, traditionally unprotected, communication services (and equipment owners) would be avoided.

In order to clarify that, as modified, S. 1667 is not intended to affect communications services other than cellular and digital transmissions, Tandy similarly proposes that Section 101(b) of S.1667 be revised to incorporate the following exceptions:

> (g) It shall not be unlawful under this chapter for any person
>
> (i) to intercept an electronic communication made through an electronic communications system designed so that such electronic communication is readily accessible to the public or, except as provided in subsection (a) hereof, historically has been accessible to the public.
>
> . . .
>
> (ii) to intercept any electronic communication which is transmitted -
>
> . . .
>
> (II) by a walkie-talkie or a police or fire communication readily, or historically, accessible to the public.
>
> . . .

In this manner, the subcommittee could ensure that the pending legislation does not inadvertently impair the public's right to use its receiving equipment.

Preliminary Statement of

Perry F. Williams

Secretary of The American Radio Relay League, Incorporated

on

Bill S.1667--"The Electronic Communications Privacy Act of 1985"

Presented
December 1985

The American Radio Relay League, Incorporated is the national, non-profit organization representing the interests of the more than 400,000 amateur radio operators licensed in the United States by the Federal Communications Commission. The League is appreciative of the opportunity to submit to this Subcommittee the views and concerns of amateur radio operators relative to the instant proposed legislation.

The Amateur Radio Service is allocated various radio frequency bands for local, regional, national and worldwide communications. Such communications promote technical self-training and provide a unique ability to enhance international goodwill. More importantly, however, amateurs are expected to and do provide regular public service and emergency communications. In every major disaster, amateur radio operators provide communications where other facilities are destroyed or overtaxed. Most recently, following the earthquake in Mexico City, and the various hurricanes along the southern and east coasts of the United States, rescue efforts were coordinated via amateur radio and literally tens of thousands of health and welfare messages were exchanged by amateur radio links. Every day, amateur radio operators put armed services and government personnel in touch with their families in the United States when otherwise such communications would be impossible. Networks of amateurs who relay messages are responsible for obtaining medical supplies on short notice for people who would not survive without it. The Federal Communications Commission has termed such operation a "priceless public benefit." In addition, amateurs have developed networks of computer data banks known as "packet networks" accessed by, and linked together with, amateur radio stations. These provide extremely rapid and error-free computer communications.

Because there are more than one and one-half million radio amateurs operating worldwide, using the same bands of radio frequencies, no one communicating via amateur radio or via amateur radio frequencies has any reasonable expectation of privacy. United States v. Sugden, 226 F.2d 281 (9th Cir. 1955) (dictum), aff'd 351 U.S. 916 (1956). A reasonable person would not expect that words uttered over an amateur radio frequency would be heard only by those few individuals for whom the communication was specifically intended. United States v. Hill, 50 Pike & Fischer Radio Regulations 2d 1331 (U.S. Court of Appeals, 1st Cir. 1982). All amateur radio operators may use any of the channels allocated to the Service (subject to transmitting restrictions based on operator license class). Thus, those utilizing amateur radio frequencies do not enjoy any expectation of privacy. See H.R. Conf. Report No. 97-765, 97th Cong., 2d Sess. at 60 (1982); reprinted in 1982 U.S. Code Cong. & Ad. News 2261. In 1982, Congress amended then §605 (now §705) of the Communications Act, 47 U.S.C., so as to clarify the absence of any expectation of privacy in connection with amateur communications and thus the exemption from the reception and disclosure restrictions of 47 U.S.C. §705.

The creation of an expectation of privacy in amateur radio is further unnecessary and antithetical to the nature of the Service. The FCC Rules and Regulations governing the Amateur Radio Service (Title 47, CFR Part 97) prohibit business communications (See §97.110); prohibit the transmission of messages for hire, or for material compensation, direct or indirect, paid or promised (See §97.112); and prohibit third-party traffic involving material compensation to any person and traffic consisting of business communications on behalf of any party (See §97.114). The Radio Regulations (Geneva 1982) require that transmissions between amateur radio stations of different countries, when permitted, must be limited to "messages of a technical nature relating to tests, and to remarks of a personal character for which, by reason of their unimportance, recourse to the public telecommunications service is not justified." Section 97.111 of the FCC Rules reiterates this treaty requirement. There are, of course, exceptions to these prohibitions relating to disaster communications. The instant Bill, however, wisely also contemplates exempting disaster communications from privacy considerations. Accordingly, no legitimate amateur radio communications demand the protection afforded by the Privacy Act.

The instant Bill would, inter alia, vastly expand the present wiretap and oral communication interception prohibitions of Chapter 119 of Title 18, United States Code, to include "electronic communications" generally. The Bill does, however, contain a provision which purportedly exempts amateur radio communications from the general prohibition of electronic communication interception. Subsection 2511(2)(g) would read, in part, as follows:

> (g) It shall not be unlawful under this chapter for any person --
>
> * * * * *
>
> (ii) to intercept any electronic communication which is transmitted --
>
> * * * * *
>
> (III) by an amateur radio station operator or by a citizens band radio operator; . . .

In addition to the above, there are other provisions within Subsection 2511(2)(g) which could be construed to exempt amateur radio communications from the proscriptions of the Bill.

Provided that the specific exemption for amateur radio communications remains in the Bill and that the same is construed and intended to apply to all forms of communication by, between and among licensed amateur stations on frequencies allocated to the Amateur Radio Service, then the League's most basic concerns are essentially satisfied. Discussions with Subcommittee staff, however, yield concerns that the Bill may be interpreted to preclude or limit the ability of amateurs to monitor those amateur radio communications involving telephone interconnect, in which one party to the amateur communications speaks and listens through a telephone line "patched" to an amateur radio transmitter and receiver. It is via these "phone patches" that amateurs put overseas servicemen in touch with their families, notify police, fire and ambulance services of emergencies, notify the Coast Guard of ships in distress, and initiate and terminate health and welfare message traffic. Phone patching has been an integral part of amateur radio emergency and public service communications since at least the Korean War, when amateurs provided communications for wounded military personnel aboard hospital ships in the Far East. The propriety thereof has been acknowledged by the Federal Communications Commission. See Carter v. AT&T Co., 13 FCC 2d 420, 13 Pike & Fischer Radio Regulations 2d 597 (1968).

Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems, are certainly not those to which this "privacy of communications" legislation is aimed. It is thus respectfully requested that any report language to accompany this legislation clearly state that all amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Service are exempt from the electronic communications intercept prohibitions of the Bill. If in the opinion of the Subcommittee the present language of the Bill does not sufficiently exempt all amateur radio communications, then the same should be amended to include, for example, an exemption for electronic communications transmitted "on frequencies allocated to the Amateur Radio Service" or the like.

Finally, it should be noted that amateurs, in performing their public service functions, occasionally utilize communications of other services, such as NOAA weather broadcasts and the like. As such, many amateurs employ "scanner" receivers which are capable of receiving communications of many different radio services (including amateur VHF and UHF communications, typically). The League is concerned that the possession of, as an example, a multiband radio receiver by a licensed amateur not subject the amateur to criminal prosecution or harassment in any fashion. Amateurs have legitimate reason to monitor frequencies outside the amateur bands. Many amateurs, for instance, are enrolled in the Military Affiliate Radio System and the Civil Air Patrol, which use frequencies assigned to the Department of Defense. Others are members of the Coast Guard Auxiliary using frequencies in the Maritime Service allocation. Some 30,000 amateurs are part of Skywarn, a system operated by the National Weather Service for tracking and warning of severe weather conditions, e.g., tornadoes; at times it may be required that they monitor Government frequencies in connection with this work. In short, there is legitimate reason for amateurs to have equipment which tunes beyond amateur bands. Amateurs must not be exposed to well-meaning but uninformed enforcement activities under the proposed Title 18 revisions. Overall, it would appear that the Bill does not contain sufficient exemptions for legitimate users of radio spectrum.

On behalf of the more than 400,000 amateur radio operators of the United States, I thank you very much for the opportunity to participate in this hearing.

CORRESPONDENCE

PERSONAL
RADIO
STEERING
GROUP
P.O. Box 2851
Ann Arbor, Michigan 48106
313/769-1616

November 25, 1985

The Honorable Charles Mathias
c/o Subcommittee on Patents, Copyrights, and Trademarks
Senate Committee on the Judiciary
137 Dirksen Senate Office Building
The United States Senate
Washington, DC 20510

In Re:
S. 1667, "Electronic Communications Privacy Act of 1985"

Dear Sir:

The Personal Radio Steering Group, Inc. is the national user representative body for citizen licensees of the General Mobile Radio Service ("GMRS"), formerly known as Class A of the Citizens Radio Service. There are more than 30,000 licensees in this personal radio service. The legislation being proposed would significantly impact their lawful communications operations to the detriment of these users and to the detriment of FCC enforcement activities.

This letter is being written to express to you our opposition to this legislation, and to raise points that have not been presented to you before, or indeed which have been concealed from you by others who have previously addressed this Subcommittee.

Statement on S. 1667 by the Personal Radio Steering Group, Inc.

CELLULAR TELEPHONE PRIVACY: WHAT IS THE REAL ISSUE?

Spokesparties for the cellular radio telephone industry are seeking new federal legislation ostensibly to obtain greater privacy of electronic communications. The legislation which has been proposed in S. 1667 would, if passed into law, make criminals out of millions of American citizens who now enjoy recreational monitoring of the very same radio waves which permeate their homes and their physical persons.

The legislation as being proposed *would not accomplish the objectives* which they seek.

The real problem of security of radio communications, if indeed it even exists in the proportions being claimed by advocates of this legislation, results from the communications industry's failure to implement certain state–of–the–art technologies. Specifically, more spectrum–efficient modulation modes are now available which utilize digital encryption techniques as an *inherent* modulation scheme. Further encryption of such modulated signals to achieve extremely high degrees of privacy can be readily accomplished *with negligible additional expense*.

Other countries are already considering and implementing such technologies, because of their demonstrated superior performance capabilities. Amongst other advantages, these new digital technologies achieve *a responsible, more efficient use* of radio spectrum which then frees up more of this valuable resource for allocation to other much–needed services currently being denied or limited because of the alleged unavailability of this resource.

The domestic communications industry, and the cellular radiotelephone industry in particular, has steadfastly refused to implement these more efficient and responsible technologies. If the cellular telephone industry truly professes such a concern about privacy, it should first certainly be expected to incorporate such technological changes as this one.

However, the motives of the communications industry are *more than slightly suspect*. One of the benefits which then accrues to the current industry interests by this continuing overconsumption of the limited resource of radio spectrum is the blocking out of new communications modes and services which these currently established interests perceive as threatening their individual communications niches, and thus their continuing market control.

France, Germany, and the Scandinavian countries, by comparison, are pursuing a much more aggressive implementation of these new, more spectrum-efficient, and more privacy-capable technologies. The "CEPT Digital Cellular Standard" for cellular telephone communications represents a significant advance in technology and responsible resource consumption, compared with the 40+ year old basic technology of Frequency Modulation being employed throughout most of the domestic communications industry (including cellular radio).

Current cellular communications, because of their location in the spectrum (the former upper end of the UHF TV band) and emission mode (Frequency Modulation) can be readily received on many conventional consumer television receivers and video cassette players. "Scanner receivers" for commercial and recreational monitoring are readily available. Older model scanners which do not include the frequencies allocated to cellular radio can be easily modified with inexpensive components to receive these cellular communications.

Any attempt to secure a greater degree of privacy by the prohibition of the reception of such signals would be *absolutely futile*. The provisions of this Act would be *totally unenforceable*, and completely without public support.

The cellular telephone industry itself is further complicit in the ready availability of these signals for monitoring. The "sidetone" retransmission of mobile units' signals by the respective cellular base stations results in *both* sides of the telephone conversation being readily discernible to *any* receiver monitoring that base-station frequency. This sidetone retransmission is quite unnecessary for the adequate performance of mobile telephony, and could be easily suppressed even with current hardwares and with only minimal technical readjustment.

By so doing, cellular providers would significantly reduce the incentive for unintended recipients to monitor such cellular transmissions, since only the base-station side of the conversation could be readily received! (The mobile transmission side is much more difficult to receive, because of the lower power, the lower antenna height, and the ever-changing location of the transmitter.)

Why has the cellular industry not taken this first, elementary step? There are certainly alternative measures for providing what little benefit may come from sidetone retransmission. If this industry truly professes such a concern about privacy, it should certainly be expected to incorporate such elementary steps as this one as well.

Voice encryption techniques are well established and the hardwares are inexpensively available. Encoding/decoding devices can be added to each cellular telephone for only a small fraction of the purchase cost of those phones. Why has a market for such devices not become more established? Because the users themselves, the ones whose rights to privacy this legislation purports to advance, do not perceive the lack of privacy as being of tantamount concern! So where does the cellular industry now find its justification for disrupting another major electronics industry component (recreational scanners)?

THE PARTICULAR CONSIDERATION OF THE GENERAL MOBILE RADIO SERVICE

GMRS, the *original* Class A of the Citizens Radio Service, was created in 1948. The much more widely known Citizens Band Radio Service (formerly known as "Class D of the Citizens Radio Service") was not created until 1957.

Citizens Band (or "CB") gained a much wider popularity because of the lower cost of equipment. However, GMRS is rapidly growing, and indeed currently exhibits the highest growth rate of *any* of the several dozen land-mobile radio services. (For instance, the licensing rate has increased by a factor of more than 1000% in just the last eight years.) Furthermore, in rule-making inquiries and actions which the Commission is now preparing, the GMRS is shortly expected to be reconfigured to become an even more broadly popular consumer radio service.

If the Subcommittee intends to proceed with this ill-advised legislation, then it is imperative that GMRS be exempted from its coverage. A similar exemption has already been given to the other two, more commonly known "personal radio services," CB and Amateur Radio

There are several reasons for this. First, limited FCC enforcement budgets require that the GMRS user community use "peer pressure" on errant GMRS licensees to encourage a higher degree of rules compliance. This peer enforcement is very important in the GMRS. Most GMRS personal–use licensees are "refugees from CB," persons who had previously licensed and operated in that abuse–laden CB service who subsequently switched to the more sophisticated and user–beneficial GMRS. These users are determined to keep GMRS from "going down the tubes" like CB did. Peer enforcement efforts are vital to this desire, because of the inadequacy of FCC enforcement efforts.

The legislation which you are considering would substantially frustrate this kind of peer enforcement, by prohibiting the monitoring of others' communications and taking subsequent actions.

Second, the GMRS is truly a *community resource*, a radio communications capability wherein multiple–party, common–channel conversations frequently occur. Such multiple–party exchanges are certainly necessary for the coordination of citizens' personal and family affairs. In such a communications environment, it is important that potentially involved parties be able to monitor on–going transmissions, and to intercede (under the authority of their respective FCC license grants) to contribute to these communications exchanges.

This *community nature* is well recognized by the users of this UHF personal radio service. They intuitively recognize that desires for "privacy" must be offset by the capability of this broader use of radio to enhance and to coordinate their personal and family activities.

Unlike CB and Amateur Radio, GMRS is not a "recreational" radio service. Instead, it is one which is evolving to a utilitarian family– and community–oriented resource.

The GMRS also plays a significant role in public–service activities by thousands of citizen volunteers. In the recent Dallas/Fort Worth Airport disaster, for instance, organized citizen volunteers contributed significantly to emergency management activities, and were central in collecting and coordinating special community resources for this relief effort. The local media recognized these valuable contributions, and gave great press coverage to them.

Less publicized but with far–reaching implications for contemporary American society are the growing number of Neighborhood Watch Programs in many local communities which have turned to the GMRS for their operational communications.

Because of these personal and family activities and vital *community–welfare* usage characteristics, it is imperative that GMRS be excluded from the provisions of this legislation in a manner similar to the exclusion afforded to CB and Amateur Radio, for instance in the provisions of Section 2511(2) of Title 18 USC (g)(ii)(iii). We respectfully request that such an exclusion be entered.

IN SUMMARY:

We oppose the creation of the prohibitions on functional and recreational monitoring being proposed in this legislation. We believe these proposed prohibitions to be entirely unenforceable. Furthermore, we feel that if indeed a problem exists (as alleged by backers of this legislation), the more appropriate solution should be found in changing certain basic technologies of cellular and other forms of radio, along the lines being advocated by the Federal Communications Commission, the Personal Radio Steering Group, and other responsible elements of the communications industry.

These changes would produce greater spectrum efficiency in current operations, would relieve the artificial "spectrum shortage" about which many industry sources now complain, and would free up additional spectrum for new radio services which would be more responsible and responsive to the continually evolving communications of contemporary American society.

In particular, if the Subcommittee decides to proceed anyway with this ill–conceived new legislation, we feel it is imperative that the General Mobile Radio Service be exempted in a manner similar to the exemptions provided for the other two, more widely known personal radio services (CB and Amateur Radio).

We thank you for this opportunity to bring these matters to your attention. If we can be of further assistance to you in this consideration, please feel free to call upon us.

Sincerely,

Corwin D. Moore, Jr.
Administrative Coordinator
Personal Radio Steering Group, Inc.

U.S. Department of Justice

Office of Legislative and Intergovernmental Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

25 JUN 1986

Honorable Strom Thurmond
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This letter is to advise you of the Department of Justice's position with regard to S. 2575, the Electronic Communications Privacy Act of 1986. This bill, which is identical to H.R. 4952 as recently passed by the House of Representatives, makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the staff of the Subcommittee on Patents, Copyrights and Trademarks, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of S. 2575.

Sincerely,

John R. Bolton

John R. Bolton
Assistant Attorney General

cc: The Honorable Joseph Biden, Jr.
The Honorable Charles McC. Mathias, Jr.
The Honorable Patrick Leahy

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

July 30, 1986

IN REPLY REFER TO

Honorable Strom Thurmond
Chairman, Senate Committee on the Judiciary
Washington, D.C. 20510

Dear Mr. Chairman:

This letter is in response to your request for comments of the Federal Communications Commission on S. 2575, the "Electronic Communications Privacy Act of 1986."

This bill would amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the "Wiretap Act" (hereafter "Title III") to penalize the unauthorized interception of electronic communications not widely available or even contemplated in 1968. These include communications made through the use of cellular telephones, voice and display pagers, private and public point-to-point microwave and satellite facilities, as well as such services as video teleconferencing, electronic mail and computer-to-computer data transmissions.

We have confined our review of the bill to Title I of S. 2575, "Interception of Communications and Related Matters," and especially to the radio-related issues raised by subsections (a) and (b) on "definitions" and "exceptions."

We defer to the jurisdiction and expertise of the Department of Justice regarding the law enforcement aspects of S. 2575, including the provisions of Titles II and III of the bill regarding "stored wire and electronic communications and transactional records access" and "pen registers" as well as electronic tracking devices. Thus, the degree to which S. 2575 may alter the balance between protecting privacy and accommodating law enforcement agencies is beyond the scope of our comments.

Background

We support the policy goals of S. 2575 to "enhance privacy protection, promote the development and proliferation of new communications technologies, and respond to the legitimate needs of law enforcement." See Introductory Statement of Sen. Charles Mathias, Congressional Record S8000 (daily ed. June 19, 1986). The bill seeks to accomplish its privacy protection objective by amending the technologically anachronistic communications privacy provisions of the federal wiretap law in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Outstripped by ever-expanding and merging electronic, computer and telecommunications technologies, which are increasingly linked by microwave and satellite radio signals, the existing legal framework of Title III is seriously outdated. Applying only to interception of "aural" (voice) acquisition of the contents of any "wire" or "oral" communication, Title III does not cover interception of data and other electronic transmissions. For example, with the proliferation of computers and other teleprocessing devices which communicate in non-voice modes, Title III is simply inapplicable in its current form to a large segment of the communications network, including digital, data, teletype or facsimile transmissions. The current wording of Title III therefore provides a significant loophole for the unauthorized interception of communications.

Moreover, as the Office of Technology Assessment (OTA) noted in its 1985 report Electronic Surveillance and Civil Liberties, "the existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance applications." The report noted that "[m]any innovations in electronic surveillance technology have outstripped constitutional and statutory protections, leaving areas in which there is currently no legal protection against, or controls on the use of, new surveillance devices."

The report underscored the need for legislation to extend protection against interception from solely voice transmissions to virtually all electronic communications, including "the digitized portion of telephone calls, the transmission of data over telephone lines, the transmission of video images by microwave, or by any other conceivable mix of medium and message." See Introductory Statement of Rep. Robert W. Kastenmeier, Congressional Record E4128 (daily ed. Sept. 19, 1985).

Summary of S. 2575

The result is S. 2575. The bill basically prohibits the mere interception of "electronic communications" (including "radio" communications), by either private parties or the government, unless the communication is exempted from protection. Under a critical statutory definition, the bill provides that radio communications not "readily accessible to the public" are protected against interception. These legally protected radio communications include those signals that are transmitted: 1) as scrambled or encrypted; 2) by a spread spectrum, private modulation technique; 3) "on a subcarrier or other signal subsidiary to a radio transmission;" 4) by a common carrier, including cellular telephones, but not cordless telephones or tone-only pagers; or 5) on frequencies allocated under certain FCC rules, including satellite communications (Part 25), auxiliary broadcast services (Part 74, Subparts D-F) or private operational fixed microwave service (Part 94).

Conversely, under a generic exemption, the bill provides that if an electronic communication is designed or "configured" so that it is "readily accessible to the public", then it is permissible to intercept that electronic communication.

With regard to satellite transmissions, the bill specifically exempts from its coverage, interception of the satellite transmissions of unscrambled and unencrypted network "front haul" feeds to affiliates, i.e., a satellite transmission "transmitted to a broadcasting station for purposes of retransmission to the general public" - unless done for "direct or indirect commercial advantage or private financial gain." It also exempts satellite cable programming as defined in 47 U.S.C. § 705, thus remaining neutral on the issue of home satellite dish reception of cable programming as addressed by the Cable Communications Policy Act of 1984. However, S. 2575 protects against interception of private satellite transmissions such as "backhaul" feeds from affiliates to networks, i.e., unedited footage from affiliates to networks of news, sports, or other program material.

Significantly, from the perspective of radio hobbyists as well as the Commission, the bill exempts from its coverage interception of the majority of radio signals, including

> specific types of radio communications which have traditionally been free from prohibitions on mere interception. Thus, it is permissible to intercept any radio communication which is transmitted (1) by any station for the use of the general public, or that relate(s) to ships, aircraft, vehicles or persons in distress; (2) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public; (3) by a station operating on a frequency assigned to amateur, citizens band or general mobile radio services, or (4) by any marine or aeronautical communications system. House Judiciary Committee, H. Rept. 99-147, to accompany H.R. 4952,

"Electronic Communications Privacy Act of 1986," 99th Cong., 2d Sess. at 41-42 (June 19, 1986) (hereafter "House Report").

Also exempted from coverage are interceptions to identify the source of "harmful interference to any lawfully operating station" and monitoring of shared but unscrambled frequency channels.

The bill affords no statutory protection against interception of transmissions over "the radio portion of a cordless communication that is transmitted between the cordless telephone handset and the base unit," standard mobile telephones, two-way radio services carried by non-common carriers, or tone-only paging devices. These technologies are not protected on the theory that they are "readily accessible to the public" and that users of the technologies are, or should be, aware of how easily their conversations can be intercepted by radio receivers. Therefore, they have no reasonable expectation of privacy.

In contrast, under the bill, the unauthorized interception of the radio portion of a cellular telephone call, whether or not it is encrypted, is penalized as a misdemeanor with a maximum penalty of six months imprisonment and/or a $500 fine. For a first offense interception of a non-cellular radio communication, the penalty, still imposed as a misdemeanor, is for up to one year in prison and/or a fine if it is done "not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain." Otherwise, the felony penalty for a repeated, "willful", not inadvertent violation of the statute, or one done for illegal, tortious, or commercial gain purposes, is imprisonment of up to five years, a fine, or both.

Discussion of S. 2575

We agree on the need to assure the privacy of new types of technologies now covered inadequately or not at all by the existing legal framework of Title III. Therefore, we support the privacy protection objective of S. 2575.

To better accomplish this objective, however, we do have two substantive policy recommendations which we discuss below. We also recommend two additional technical amendments, proposed report language, and a correction.

Satellite Interference

We request that an amendment be added to S. 2575 to prohibit transmissions intended to interfere with the operation of satellites, or with the transmissions which they convey. This amendment arises out of the notorious "Captain Midnight" incident this past April when an individual in Ocala, Fla. deliberately interfered with the transmission of an HBO program being relayed by the Galaxy 1 communications satellite.

Deliberate interference with satellites and the communications which they convey poses a serious threat to the integrity of our important satellite network. We believe that this amendment is necessary in order to deter the occurrence of such episodes in the future. It would exert this deterrent effect by increasing the potential penalty for such an offense from up to one year in prison, a $10,000 fine, or both, currently, to up to 10 years in prison, a $250,000 fine, or both. Finally, by putting this provision in the criminal code, the FBI and the Department of Justice would have unambiguous authority to investigate and prosecute this serious offense. Attached is a version of the proposed amendment (with Congressional Record statement) introduced as H.R. 4983 by Rep. Howard Coble on June 11, 1986.

We would be pleased to work closely with Committee staff to perfect the appropriate statutory and report language as well as address any concerns of other agencies about the amendment.

Definitions

Questions have been raised about categorizing as not "readily accessible to the public" subcarrier or subsidiary transmissions and Part 74 remote auxiliary broadcast transmissions. The Association of North American Radio Clubs (ANARC), for example, argues that these transmissions are, in fact, "readily accessible to the public" and can be tuned in by anyone with the proper equipment. We believe that these communications do deserve privacy protection but the rationale for, and scope of, their inclusion within the definition of being not "readily accessible to the public" should be clearer in the legislative history. This clarity is necessary to give sufficient guidance not only to the courts and law enforcement but especially to members of the public who may well have difficulty in determining whether or not a particular radio communication is, or is not, "readily accessible to the public." In this regard, it appears that the House Report, at 37, addresses at least part of ANARC's concern about the inclusion of subcarrier or subsidiary transmissions within the not "readily accessible" definition. It clearly states that "it is not unlawful to intercept subcarrier and VBI (vertical blanking interval) communications that are transmitted for the use of the general public, *e.g.*, the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of television programming for the hearing-impaired." Presumably, other material transmitted on subcarriers intended for public reception would also be permitted, as our rules permit such use. Report language should so indicate. Finally, to emphasize this clarification, it would be preferable to insert it in the bill as well as in report language.

Technical Amendments

1. Page 7, lines 5-7:

Change:

> "(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services"

to:

> "(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services."

Explanation

Neither the amateur nor citizens band radio services are "assigned" frequencies as that term is generally used in communications law. Rather, "bands" or "pairs" of contiguous frequencies are "allocated" for their use. Licensees may use at will any of the frequencies within the allocated limits. General mobile radio services are also allocated frequency bands but with frequency assignments still made within the allocation.

2. Page 7, lines 18-20:

Change:

> "[in]terference to any lawfully operating station, to the extent necessary to identify the source of such interference;"

to:

> "[in]terference to any lawfully operating station, or consumer electronic equipment."

Explanation

As currently drafted in S. 2575, this proposed exception would allow interception of any wire or electronic communication "causing harmful interference to any lawfully operating station," only "to the extent necessary to identify the source of such interference."

We propose two amendments to this exception. First, we believe this exception should be broadened to include transmissions interfering with home, consumer electronic devices and equipment, such as televisions, VCRs, record players and telephones. Such interference is a very common complaint, so much so that in 1982, Congress recognized that radio frequency energy can interfere with home electronic systems and equipment and explicitly authorized the Commission to regulate radio frequency interference with consumer electronic equipment. See P.L. 97-259, 47 U.S.C. sec. 302. It should not be illegal for an individual to tune into an interfering signal from a nearby cellular radio source, for example, because the interference is to his or her record player rather than to a "lawfully operating station."

Second, we propose deleting "to the extent necessary to identify the source of such interference." As the Association of North American Radio Clubs (ANARC) pointed out in a letter dated July 14, 1986 to Senator Patrick J. Leahy:

"The FCC relies to a great extent on citizen complaints in administrative proceedings against stations causing interference. The definition of 'harmful interference' used in most cases is given in 47 CFR 2.1:

> 'interference which...seriously degrades, obstructs, or repeatedly interrupts a radio communications service operating in accordance with these Radio Regulations.' [emphasis added]

If it were lawful to monitor an interfering signal only until its source is identified, and if the source were a transmitter of communications protected by S. 2575, citizens would face criminal liability in establishing or reporting that the interference is causing them repeated interruptions in service. This would make it difficult for the FCC to obtain evidence against the most serious violators of the right of non-interference, the right which is the basis of radio regulation in this country and internationally.

To avoid this clearly undesirable and unnecesssary result, we recommend that the phrase, '...to the extent necessary to identify the source of such interference' be stricken from section 2511(2)(g)(iv). If the Subcommittee wishes to differentiate between 'electronic' and 'wire' communication on this point, we would have no problem with that."

Report Language

In its letter of July 14, 1986 to Senator Leahy, ANARC raises two additional points, both of which we believe could be adequately addressed in appropriate report language.

1. Environmental Monitoring

As ANARC points out, both the FCC and EPA, as well as an increasing number of state and local governments, are currently addressing the problem of potentially excessive public exposure to radio frequency (RF) radiation emitted by various transmitting antennas, especially FM radio transmitters. For example, under an environmental processing guideline adopted in March, 1985, and effective January, 1986, the FCC is now routinely evaluating human exposure to RF radiation as an environmental issue when it considers applications to construct, license, renew, or modify TV, radio, low-power TV, experimental radio and transmitting satellite-earth stations.

However, the FCC is proposing to exclude categorically the majority of common carrier and private radio transmitters from RF radiation regulation. These include cellular mobile radios, point-to-point microwave relay stations, land mobile radios, paging services, amateur radio facilities, aviation and marine stations, digital electronic message and multipoint distribution services. The Commission has proposed the categorical exclusion of these transmitting sources because of a lack of current evidence that they present a potential radiation hazard to the public. In particular, it cites their lower operating power, intermittent use, high directionality of the transmitted energy beam, and relative inaccessibility to the general public.

The FCC's new RF radiation guideline will, however, have some immediate impact on the non-broadcast industry, especially terrestrial, transmitting satellite-earth stations.

S. 2575 would make it unlawful to intercept satellite communications governed by Part 25 of the FCC Rules. ANARC is correct that "to the extent the primary relevant measurements [of RF radiation] are frequency and field strength, there is no need to 'intercept' (acquire the contents of) the transmission." However, it is also true that to establish the actual source of RF radiation, it may be necessary to intercept the emission, especially in the case of "antenna farms" with multiple sources of RF emissions.

Therefore, we agree that the Committee should address this question in its consideration of S. 2575. However, we believe the matter can be addressed adequately with the following report language rather than in an amendment to the bill:

> "By defining satellite communications regulated under Part 25 of the FCC's Rules to be not 'readily accessible to the general public' and therefore protected against unauthorized interception, the Committee does not intend to prohibit the necessary interception of a satellite transmission solely to determine the source of a radio frequency (RF) emission in order to comply with or enforce applicable federal or state standards limiting human exposure to RF radiation."

2. Surreptitious Interception

On page 8, lines 20-25, of S. 2575 a technical amendment is made to substitute "wire, oral, or electronic" for "wire or oral" in a number of sections of the Wiretap Act, including sections 2512 and 2513. The amendment to these sections would make it a crime to mail, advertise, manufacture, assemble, possess or sell any device the design of which "renders it primarily useful for the purpose of the surreptitious interception of...electronic...communications."

Since "electronic" communication includes "radio" receivers, we agree with ANARC that the terms "primarily useful" and "surreptitious" should be clarified. For example, would this language ban equipment currently on the market and widely used that receives 15-30 MHz, or 50-500 MHz? Would the language ban or restrict scanning receivers ("scanners"), general coverage receivers, and subcarrier tuners? Would radios primarily designed for indoor use, not visible to the outdoor public, be deemed "surreptitious"?

Neither the bill nor the House Report */ addresses these questions. Therefore, further clarification of the intended scope of the terms would be helpful.

---

*/ In fact, the only relevant discussion of scanners in the House Report is a general statement that "the Committee finds [the capability of newer scanners to receive cellular frequencies] troubling and expects that the future design and manufacture of scanners will take into account the privacy protections accorded cellular telephony in this legislation." House Report, at 32.

Technical Correction

Page 43, last paragraph, line three, House Report:

Change "2511(4)(b)(iii)" to "2511 (4)(c)."

Explanation

This is a technical error. There is no 2511(4)(b)(iii) subsection in either H.R. 4925 or S. 2575. The correct citation should be "2511(4)(c)."

Conclusion

As we have stated, we support the privacy protection objective of S. 2575. We believe the legislation, if amended, may offer a reasonable and responsible statutory basis for deterring unauthorized interception of new radio and other electronic communications technologies and therefore contribute to the full development and use of these technologies.

Thank you for the opportunity to comment on this legislation. If we can be of any further assistance to the Committee in its consideration of S. 2575, please contact us.

Sincerely,

William A. Russell, Jr.
Director, Office of Congressional and
Public Affairs

Attachment

ATTACHMENT

99TH CONGRESS
2D SESSION

H. R. 4983

To amend chapter 65 of title 18, United States Code, to provide a criminal penalty for interference with satellite communications.

IN THE HOUSE OF REPRESENTATIVES

JUNE 11, 1986

Mr. COBLE (for himself and Mr. FRANK) introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To amend chapter 65 of title 18, United States Code, to provide a criminal penalty for interference with satellite communications.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Satellite Communications Protection Act of 1986".

SEC. 2. CRIMINAL PENALTY FOR INTERFERENCE WITH SATELLITE COMMUNICATIONS.

Chapter 65 of title 18, United States Code, is amended by adding at the end the following new section:

"§ 1365. Interference with satellite communications

"Whoever willfully or maliciously interferes with the operation of a communications satellite or obstructs, hinders, or delays any transmission conveyed by means of a communications satellite shall be fined in accordance with this title or imprisoned not more than ten years, or both.".

SEC. 3. TECHNICAL AMENDMENT.

The table of sections for chapter 65 of title 18, United States Code, is amended by adding at the end the following new item:

"1365. Interference with satellite communications.".

○

CONGRESSIONAL RECORD — *Extensions of Remarks*

CAPTAIN MIDNIGHT

HON. HOWARD COBLE

OF NORTH CAROLINA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, June 11, 1986

Mr. COBLE. Mr. Speaker, on April 27, at 12:30 a.m. eastern time, a video pirate, calling himself Captain Midnight, interrupted the satellite transmission of the cable television service Home Box Office. The interruption lasted only 5 minutes, but it was an incident that could have long-term effects. It was a signal that all satellite transmissions—including those by Government, defense, and private satellite—are vulnerable to sabotage.

Current law is insufficient to deal with these video terrorists who seek to intercept or disrupt satellite transmissions. That is why today I am introducing the Satellite Communications Protection Act of 1986. This bill is a simple solution to a complex problem. Right now, the penalties for anyone convicted of interfering or obstructing a non-Government satellite transmission are not sufficient to act as a deterrent. My bill would amend chapter 65 of title 18 of United States Code, to increase the maximum prison term for anyone convicted of interfering with satellite communications from 1 year to 10 years. The maximum possible fine will remain at $250,000.

I am pleased to report that Congressman BARNEY FRANK of Massachusetts has agreed to cosponsor this bill in the House. The legislation will be sent to the Judiciary Committee. Similar legislation will be introduced in the Senate.

With prison terms up to 10 years, and fines up to a quarter million dollars, we feel that we will have the proper deterrent to thwart those who seek to interrupt satellite activity. The Captain Midnight episode, involving HBO is just the tip of the iceberg in possible video terrorism. The FCC has received information that deliberate interference of satellite transmission is being encouraged. There are more than two dozen commerical U.S. satellites now in orbit, along with several weather, military, and space agency satellites.

Most experts agree that the vast majority of these satellites are vulnerable to rather easy access by people using relatively inexpensive equipment. The Federal Government, which uses satellites for all types of communications, is exposed to possible tampering. Attorney General Edwin Meese has requested that the Justice Department investigate any cases of satellite interference.

In addition to the national security and commercial implications of this problem, every consumer who uses and enjoys satellite transmissions as home entertainment should be entitled to receive signals without unlawful interference. Congress should act to protect consumers' interests. The Captain Midnights of this world are no friend to the owners of satellite dishes.

While we are introducing this bill today, we would encourage the satellite industry to continue its efforts to make its product less vulnerable to disruption. Until satellites can be developed that are tamperproof, an increase in the penalties for those who do the tampering is the next best step. I am hopeful that this bill will move swiftly through Congress so that we can stop the spread of video terrorism before it becomes more of a threat to our vast system of news, weather, entertainment, broadcast networks, commercial, and military satellites.

○